RX3042H

Руководство пользователя

Содержание

Перечень рисунков

Перечень таблиц

Глава 1 Введение

Поздравляем с приобретением RX3042H. Теперь вашу локальную сеть можно подключить к Интернет, используя высокоскоростное широкополосное соединение, например ADSL модем или кабельный модем.

Это руководство расскажет вам как установить и настроить RX3042H для получения высокой производительности.

1.1 Характеристики

- LAN: 4-портовый коммутатор Fast Ethernet
- WAN: два 10/100Base-T Ethernet порта предоставляют доступ к Интернет для всех компьютеров вашей сети
- Функции Firewall, и NAT (Преобразование Сетевых Адресов) обеспечивают безопасный доступ к Интернет для вашей сети
- Автоматическое назначение сетевых адресов через сервер DHCP, включая настройку IP маршрутизации, DNS и DDNS
- Настройка через браузер, например Microsoft Internet Explorer 6.0 или новее.
- Поддержка пользовательской настройки два WAN или WAN плюс DMZ
- Поддержка USB (будет поддерживаться с обновлением прошивки)

1.2 Системные требования

Для доступа к Интернет, используя RX3042H, вам нужно иметь следующее:

- ADSL или кабельный модем с доступом к Итернет и хотя бы один интернет адрес, назначенный для вашей сети
- Один или более компьютеров с сетевыми адаптерами (NIC) Ethernet 10Base-T или 100Base-T или 1000Base-T
- (дополнительно) Ethernet хаб/коммутатор, если вы хотите подключить роутер к более чем четырем компьютерам в сети Ethernet.
- Для настройки системы, используется GUI: браузер Internet Explorer 6.0 или новее.

1.3 Использование этого документа

1.3.1 Соглашения

- Акронимы, определенные сначала, появляются в тексте.
- Для краткости, иногда будем называть RX3042H как “роутер” или ”шлюз”.
- Термины LAN и network используются для обозначения группы компьютеров, соединенных Ethernet.
- Последовательность действий мышью обозначена символом “->”. Например, **System -> Network Setup** означает щелкните меню **System** и затем щелкните подменю **Network Setup**.

1.3.2 Типографские соглашения

- Жирный шрифт используется для пунктов, которые вы выбираете в меню и списках, и данных, которые вы вводите.

1.3.3 Специальные сообщения

В этом документе используются следующие значки для привлечения вашего внимания к инструкциям или объяснениям.



Примечание: Предоставляет объяснение или дополнительную информацию к текущей теме.



Определение: Объясняет термины или акронимы, которые могут быть не знакомы читателям. Эти термины также включены в глоссарий.



Внимание: Предоставляет важные сообщения, включая сообщения, связанные с личной безопасностью или с целостностью системы.

Глава 2 Знакомство с RX3042H

2.1 Комплект поставки

Вместе с этим документом поставляется следующее:

- Роутер
- Блок питания
- Ethernet-кабель ("прямого" типа)

2.2 Аппаратные функции

LAN

- 4-х портовый коммутатор Fast Ethernet
- Автоматическое определение скорости

WAN

- Два 10/100M Ethernet порта
- Автоматическая поддержка MDI/MDIX

2.3 Программные функции

2.3.1 Функция NAT

RX3042H предоставляет NAT для разделения высокоскоростного подключения к Интернет и позволяет сохранить стоимость множества подключений требуемых для узлов в сегменте сети. Эта функция скрывает сетевой адрес и препятствует ему становиться достоянием общественности. Она преобразует незарегистрированные IP адреса узлов, подключенных к сети в правильный для доступа к Интернет. RX3042H также предоставляет возможность обратного NAT, предоставляя пользователям различные службы, например сервера e-mail, web и т.п. Правила NAT управляют механизмом преобразования. RX3042H поддерживает следующие типы NAT.

- NAPT (трансляция сетевого адреса и порта)– Также называемый маскирующий IP или ENAT (Расширенный NAT). Отображение многих внутренних узлов на один общий IP адрес. Обычно отображение

содержит пул сетевых портов, используемых для трансляции. Каждый пакет транслируется с общим IP адресом; номер порта транслируется с помощью свободного пула из пула сетевых портов.

- Обратный NAPT – Также называемый входящим распределением, распределением портов или виртуальным сервером. Любой пакет, приходящий к роутеру может быть передан внутреннему узлу, основываясь на протоколе, номере порта и/или IP адресе, определенных в правилах. Это полезно когда много служб работают на различных внутренних узлах.

2.3.2 Функции брандмауэра

Брандмауэр, встроенный в RX3042H обеспечивает следующие возможности для защиты вашей сети от атак и предотвращает подключение злоумышленников к вашей сети.

- Динамическая фильтрация пакетов
- Статичекая фильтрация (ACL)
- Защита от DoS-атак
- Журнал

2.3.2.1 Динамическая фильтрация пакетов

Брандмауэр RX3042H использует “динамическую фильтрацию пакетов” , которая извлекает информацию из пакета и сохраняет эту информацию для оценки попыток последующих соединений. Это создает динамические подключения так, чтобы никакие порты не были открыты кроме необходимых. Это предоставляет безопасное решение, которое обеспечивает масштабируемость и расширяемость.

2.3.2.2 Статическая фильтрация–ACL(Список контроля доступа)

Правила ACL одно из основных действий для сетевой безопасности. Брандмауэр проверяет каждый пакет в сети, декодирует информацию заголовка и затем разрешает или блокирует этот пакет, основываясь на содержании исходного адреса, адреса назначения, исходного порта, порта назначения и протокола, определенных в правилах ACL.

ACL очень подходит для обеспечения изоляции одной подсети от другой. Это может использоваться как первая линия защиты для блокировки

пакетов определенных типов.

Брандмауэр RX3042H поддерживает следующие методы ACL:

- Фильтрация, основанная на исходном адресе, адресе назначения, исходном порту, порте назначения и протоколе
- Использование групп для правил фильтрации
- Приоритеты фильтрации

2.3.2.3 Защита от DoS атак

Брандмауэр RX3042H имеет механизм защиты от атак, который защищает внутреннюю сеть от известных типов интернет-атак. Это обеспечивает автоматическую защиту от DoS атак, таких как SYN flooding, IP smurfing, LAND, Ping of Death и всех фрагментированных атак. Например, брандмауэр RX3042H обеспечивает защиту от “WinNuke”, широко используемая программа для удаленного разрушения незащищенных систем Windows в Интернет. Брандмауэр RX3042H также обеспечивает защиту от различных широкоиспользуемых интернет-атак, например IP Spoofing, Ping of Death, Land Attack и фрагментированных атак.

Типы атак от которые обнаружаются RX3042H представлены в таблице 2.1.

Таблица 2.1. DoS атаки

Тип атаки	Название атаки
Фрагментированные атаки	Bonk, Boink, Teardrop (New Tear), Overdrop, Opntear, Syndrop, Jolt, перекрытие фрагментации IP.
ICMP атаки	Ping of Death, Smurf, Twinge
Наводнения	Регистрируются только ICMP Flooder, UDP Flooder, SYN Flooder
Сканирование портов	Регистрируются только TCP SYN Scan, Attacking packets dropped: TCP XMAS Scan, TCP Null Scan, TCP Stealth Scan
Защита с помощью PF правил	Echo-Chargen, Ascend Kill
Смешанные атаки	IP Spoofing, LAND, Targa, Winnuke

2.3.2.4 Шлюз уровня приложения (ALG)

Приложения типа FTP динамически открывают подключения, основываясь на соответствующих параметрах приложения. Для прохождения через брандмауэр RX3042H, пакетам, относящимся к приложениям, требуются соответствующие разрешающие правила. При отсутствии таких правил, пакеты будут отброшены брандмауэром RX3042H. Поскольку невозможно создать политику для многочисленных приложений динамически (одновременно не ставя под угрозу безопасность), интеллектуальный шлюз уровня приложения (ALG) выполняет разбор пакетов для приложений и открывает динамические ассоциации. RX3042H NAT предоставляет номер ALG для популярных приложений типа FTP и Netmeeting.

2.3.2.5 Журнал

События в сети, которые могут повлиять на безопасность, записываются в системный журнал RX3042H. Журнал поддерживает минимум деталей например, время прибытия пакета, описание действий брандмауэра и причина этих действий.

2.4 Осмотр роутера

2.4.1 Передняя панель

На передней панели расположены индикаторы, показывающие состояние устройства.

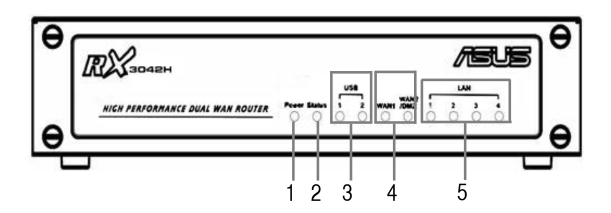


Рис. 2.1 Передняя панель

Таблица 2.2 Индикаторы передней панели

	Название	Цвет	Состояние	Описание
1	Питание	зеленый	горит	RX3042H включен.
			не горит	RX3042H выключен.
2	Состояние	зеленый		
3	USB			Состояние портов USB.
	1-2	зеленый	не горит	устройство USB не обнаружено.
			горит	устройство USB обнаружено.
4	WAN1 и WAN2/DMZ		не горит	Нет связи.
		зеленый	горит	Установлена связь100Mbps.
			мигает	Передача данных 100Mbps.
		желтый	горит	Установлена связь10Mbps.
			мигает	Передача данных 10Mbps.
5	LAN			Состояние портов LAN.
	1-4		не горит	Нет связи.
		зеленый	горит	Установлена связь100Mbps.
			мигает	Передача данных 100Mbps.
		желтый	горит	Установлена связь10Mbps.
			мигает	Передача данных 10Mbps.

2.4.2 Задняя панель

На задней панели находятся порты для устройств и разъем питания.

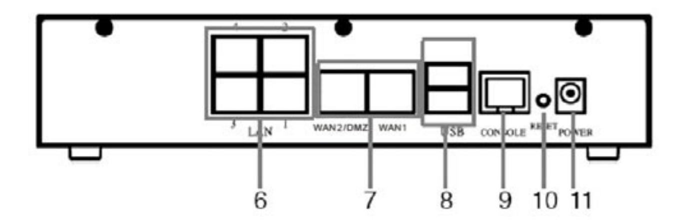
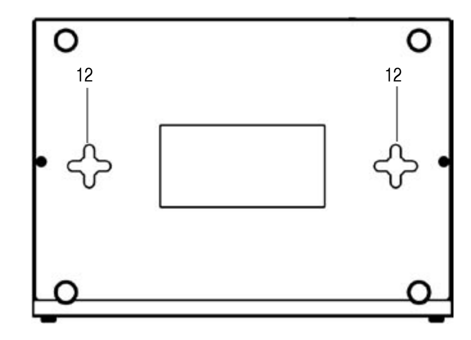


Рис. 2.2 Задняя панель

Таблица 2.3 Задняя панель

	Обозначение	Описание
6	1--4	Порты LAN: для подключения ваших ПК и/или хабов/коммутаторов с помощью кабеля Ethernet.
7	WAN1 and WAN2/DMZ	Два порта WAN или 1 WAN + 1 DMZ: для подключения устройств WAN, типа ADSL модема или кабельного модема или сети DMZ. Пожалуйста имейте в виду, что сеть DMZ должна быть подключена к порту WAN2/DMZ.
8	USB	Порты USB: для подключения устройств USB 1.1 или 2.0
9	Console	Не поддерживается.
10	RESET	Кнопка сброса: 1. Перезагрузка устройства 2. Сброс к заводским установкам, если нажать и удерживать кнопку более 5 секунд.
11	POWER	Разъем питания: для подключения блока питания.

2.4.3 Нижняя панель



12. Монтажные скобы: Для экономии места вы можете повесить RX3042H на стену. В зависимости от ваших конкретных требований, принимая во внимание расположение розетки питания, длины шнура питания, длины кабелей и т.д., вы можете повесить RX3042H в 4 различных ориентациях: передней панелью вверх, задней панелью вверх, левой панелью вверх или правой панелью вверх.

2.5 Размещение

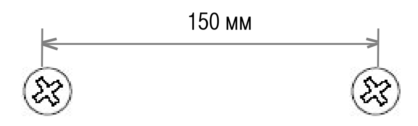
В зависимости от ваших условий, вы можете выбрать один из двух способов размещения RX3042H – настольное размещение или настенное размещение.

2.5.1 Настольное размещение

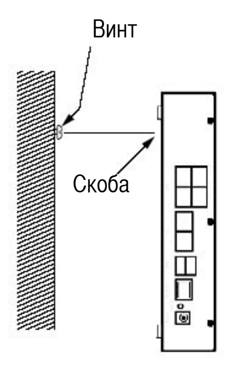
Вы можете поместить RX3042H на любую ровную поверхность. Дизайн RX3042H занимает немного места на вашем столе.

2.5.2 Инструкции для настенного размещения:

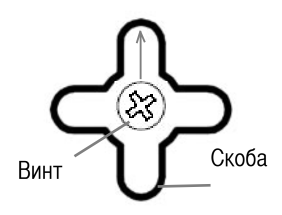
1. Закрутите два винта в стену на расстоянии 150 мм и убедитесь, что винты выровнены.



2. Поместите монтажные скобы роутера напротив винтов и повесьте роутер так, чтобы оба винта были вставлены в ответстия скоб, как показано на рисунке. Роутер поддерживает 4 вида размещения на стене: передней панелью вверх, задней панелью вверх, левой панелью вверх или правой панелью вверх.



Поместите монтажные скобы роутера напротив винтов



Повесьте роутер так, чтобы оба винта были вставлены в ответстия скоб и затем медленно толкните роутер вниз, как показано на рисунке выше.

3 Руководство по быстрой установке

Это руководство по быстрой установке предоставляет основные инструкции для подключения RX3042H к компьютеру или сети и к Интернет.

- В части 1 представлены инструкции по установке оборудования.
- В части 2 описано как настроить Интернет на вашем компьютере(ах).
- В части 3 показано как сконфигурировать основные настройки RX3042H для подключения вашей сети к Интернет.

После настройки устройства, вы можете следовать инструкциям на странице 15 для проверки что все работает правильно.

Это руководство по быстрой установке подразумевает, что вы уже имеете соединие с вашим провайдером(ISP), установленное с помощью ADSL модема или кабельного модема. Эти инструкции обеспечивают основную конфигурацию, которая должна быть совместима с домашней или небольшой офисной сетью. В последующих частях представлены инструкции для дополнительной настройки.

3.1 Часть 1 — Подключение оборудования

В 1-ой части, мы подключим устройство к ADSL модему или кабельному модему (который подключен к телефонной и кабельной линии), розетке питания и вашему компьютеру или сети.



Внимание: Переда началом установки выключите все устройства. Это включает ваш компьютер(ы), хаб/коммутатор (если используется) и RX3042H.

На рисунке 3.1 показано подключение оборудования. Пожалуйста следуйте следующим инструкциям.

3.1.1 Шаг 1. Подключение ADSL или кабельного модема

Для RX3042H: подключите один конец кабеля Ethernet к порту с обозначением WAN на задней стороне устройства. Подключите другой конец к порту Ethernet вашего ADSL модема или кабельного модема.

3.1.2 Шаг 2. Подключение компьютеров или сети.

Если в вашей сети не более 4 компьютеров, вы можете использовать кабель Ethernet для прямого подключения компьютеров к устройству. Имейте в виду, что вам следует подключить один конец сетевого кабеля к любому порту помеченному цифрами 1 – 4 на задней стороне роутера, а другой конец к сетевому порту компьютера.

Если в вашей сети более 4 компьютеров, вы можете подключить один конец кабеля к хабу или коммутатору (вероятно к входному порту; пожалуйста смотрите документацию на хаб/коммутатор), а другой конец к порту (отмеченному 1 – 4) на задней стороне RX3042H.

Имейте в виду, что для подключения к роутеру компьютеров, хабов или коммутаторов можно использовать любой(прямой или перевернутый) сетевой кабель.

3.1.3 Шаг 3. Подключение блока питания.

Подключите блок питания к разъему POWER на задней стороне устройства и подключите его к настенной розетке.

3.1.4 Шаг 4. Включение RX3042H, ADSL- или кабельного модема и ваших компьютеров

Подключите блок питания к гнезду питания RX3042H. Включите ваш ADSL модем или кабельный модем. Включите и загрузите ваш компьютер(ы) и/или другие сетевые устройства(беспроводные точки доступа, хабы или коммутаторы).

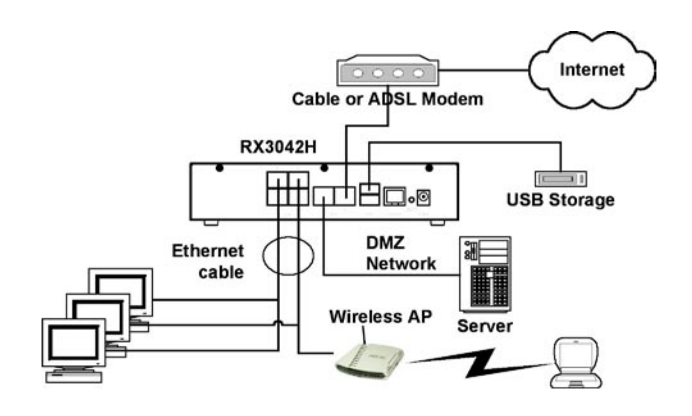


Рис. 3.1 Обзор соединений

Вам следует проверить, что индикаторы горят как указано в таблице 3.1.

Таблица 3.1 Индикаторы

Индикатор:	**...должен быть:**
POWER	Зеленый цвет показывает, что устройство включено. Если не горит, проверьте, что блок питания подключен к RX3042H и к источнику питания.
LAN	Зеленый цвет означает, что устройство установило связь с вашей сетью и мигает, когда устройство принимает или передает данные к/от компьютеров вашей сети.
WAN	Зеленый цвет означает, что устройство успешно установило связь с вашим провайдером и мигает, когда устройство принимает или передает данные в/из Интернет.

Если индикаторы горят как указано, RX3042H работает правильно.

3.2 Часть 2 — Настройка ваших компьютеров

Во 2-ой части Руководства по Быстрой Установке предоставлены инструкции по настройке ваших компьютеров для работы с RX3042H.

3.2.1 Приступая к настройке

По умолчанию, RX3042H автоматически предоставляет вашему ПК все необходимые параметры (IP адрес, DNS сервер, шлюз по умолчанию). Вам только нужно настроить ваш ПК для получения сетевых параметров от RX3042H.



Примечание: Иногда, вы может быть хотите настроить сетевые параметры вручную для некоторых или всех ваших компьютеров, а не получать параметры от RX3042H. Инструкции смотрите на странице 17 “Назначение статических IP адресов для ваших ПК”.

- Если вы подключили ваш ПК к RX3042H, следуйте инструкциям в соответствии с операционной системой, установленной на вашем ПК.

3.2.2 ПК с Windows® XP:

1. В панели задач нажмите кнопку <**Start**>, затем щелкните Control Panel.

2. Два раза щелкните на иконке **Network Connections**.

3. В окне **LAN or High-Speed Internet**, правой кнопкой щелкните на иконке, соответствующей вашей сетевой карте (NIC) и выберите **Properties**. (Часто эта иконка называется **Local Area Connection**).

   Появится окно Local Area Connection с перечнем установленных сетевых компонентов.

4. Проверьте, что компонент **Internet Protocol (TCP/IP)** выбран и щелкните кнопку <**Properties**>.

5. В окне **Internet Protocol (TCP/IP) Properties**, выберите **Obtain an IP address automatically**. Также выберите **Obtain DNS server address automatically**.

6. Нажмите кнопку <**OK**> дважды, подтвердив изменения и закройте **Control Panel**.

3.2.3 ПК с Windows® 2000:

Сначала, проверьте наличие протокола IP и, если необходимо, установите его:

1. В панели задач Windows, нажмите кнопку <**Start**>, выберите **Settings** и затем щелкните **Control Panel**.

2. Два раза щелкните на иконке **Network and Dial-up Connections**.

3. В окне **Network and Dial-up Connections**, щелкните правой клавишей на иконке **Local Area Connection**, затем выберите **Properties**.

   Появится окно **Local Area Connection Properties** с перечнем установленных сетевых компонентов. Если в списке есть **Internet Protocol (TCP/IP)**, значит протокол уже установлен. Перейдите к пункту 10.

4. Если **Internet Protocol (TCP/IP)** не показан как установленный компонент, нажмите кнопку <**Install**>.

5. В окне **Select Network Component Type** выберите **Protocol**, затем нажмите кнопку <**Add**> .

6. В списке протоколов выберите **Internet Protocol (TCP/IP)**, затем нажмите кнопку <**OK**>.

   Возможно появится подсказка для установки файлов с компакт-

диска Windows 2000 или другого носителя. Следуйте инструкциям для установки файлов.

7. Если появится подсказка для перезагрузки вашего компьютера с новыми параметрами, нажмите кнопку <**OK**>.

   Далее, настройте ПК для получения IP адресов от RX3042H:

8. В Control Panel, два раза щелкните на иконке **Network and Dial-up Connections**.

9. В окне Network and Dial-up Connections, правой кнопкой щелкните на иконке **Local Area Connection**, затем выберите **Properties**.

10. В окне Area Connection Properties, выберите **Internet Protocol (TCP/IP)**, затем нажмите кнопку <**Properties**>.

11. В окне **Internet Protocol (TCP/IP) Properties**, выберите **Obtain an IP address automatically**. Также выберите **Obtain DNS server address automatically**.

12. Нажмите кнопку <**OK**> дважды для подтверждения и сохранения ваших изменений, затем закройте Control Panel.

3.2.4 ПК с Windows® 95, 98 и ME

1. В панели задач Windows нажмите кнопку <**Start**>, выберите **Settings**, затем щелкните **Control Panel**.

2. Дла раза щелкните по иконке **Network**.

   В окне Network найдите элемент, начинающийся с “**TCP/IP ->**” и названием вашей сетевой карты, затем нажмите кнопку <**Properties**>. Если в списке есть такой элемент, значит протокол TCP/IP уже установлен. Перейдите к пункту 8.

3. Если Internet Protocol (TCP/IP) не показан как установленный компонент, нажмите кнопку <**Add**>.

4. В окне **Select Network Component Type**, выберите **Protocol**, затем нажмите кнопку <**Add**>.

5. Из списка производителей выберите **Microsoft**, затем в списке протоколов выберите TCP/IP, затем нажмите кнопку <**OK**>.

   Возможно появится подсказка для установки файлов с компакт-диска Windows 95, 98 или Me или другого носителя. Следуйте инструкциям

для установки файлов.

6. Если появится подсказка для перезагрузки вашего компьютера с новыми параметрами, нажмите кнопку <**OK**>.

   Далее, настройте ПК для получения IP адресов от RX3042H:

7. В Control Panel два раза щелкните на иконе **Network.**
8. В окне Network выберите элемент, начинающийся с “**TCP/IP ->**” и названием вашей сетевой карты, затем нажмите кнопку <**Properties**>.
9. В окне TCP/IP Properties выберите **Obtain an IP address automatically**.
10. В окне TCP/IP Properties щелкните вкладку “**Default Gateway**”. Введите **192.168.1.1** (IP адрес RX3042H по умолчанию) в поле “**New gateway**” и нажмите кнопку <**Add**> для добавления шлюза по умолчанию.
11. Нажмите кнопку <**OK**> дважды для подтверждения и сохранения ваших изменений, затем закройте Control Panel.
12. Если появится подсказка для перезагрузки компьютера, нажмите кнопку <**OK**>.

3.2.5 Windows® NT 4.0 workstations:

Сначала, проверьте наличие протокола IP и, если необходимо, установите его:

1. В панели задач Windows NT нажмите кнопку <**Start**>, выберите **Settings**, затем щелкните **Control Panel**.
2. В окне Control Panel дважды щелкните на иконке **Network**.
3. В окне Network выберите вкладку **Protocols**.

   Появится список установленных сетевых протоколов. Если в списке есть TCP/IP Protocol, значит протокол уже установлек. Перейдите к пункту 9.

4. Если TCP/IP нет в списке установленных компонентов, нажмите кнопку <**Add**> .
5. В окне Select Network Protocol выберите TCP/IP, затем нажмите кнопку <**OK**> .

   Возможно появится подсказка для установки файлов с компакт-диска Windows NT или другого носителя. Следуйте инструкциям для установки файлов.

После установки всех файлов, появится окно, спрашивающее вас использовать ли службу DHCP для динамического присваивания IP адресов.

6. Нажмите кнопку <**Yes**> для продолжения, затем нажмите кнопку <**OK**> для перезагрузки компьютера.

Далее, настройте ПК для получения IP адресов от RX3042H:

7. Откройте **Control Panel**, затем дважды щелкните на иконке **Network**.
8. В окне Network выберите вкладку **Protocols**.
9. Далее выберите **TCP/IP**, затем нажмите кнопку <**Properties**>.
10. В окне Microsoft TCP/IP Properties, выберите **Obtain an IP address from a DHCP server**.
11. Нажмите кнопку <**OK**> дважды для подтверждения и сохранения ваших изменений, затем закройте Control Panel.

3.2.6 Назначение вашим ПК статических IP адресов

Иногда, необходимо вручную назначить IP адреса для некоторых или всех ваших ПК(часто называется “statically”), а не получать их от RX3042H. Это желательно (но не требуется) если:

- У вас есть один или несколько IP адресов, которые вы всегда хотите использовать с определенными компьютерами (например, если вы используете компьютер как веб-сервер).
- В вашей сети есть различные подсети.

Тем не менее, первый раз при настройке вашего RX3042H, вы должны использовать IP адрес в сети 192.168.1.0 для вашего ПК, например 192.168.1.2, для установки соединения между RX3042H и вашим PC так как по умолчанию сетевой IP адрес RX3042H установлен как 192.168.1.1. Введите 255.255.255.0 для маски подсети и 192.168.1.1 для шлюза по умолчанию. Эти установки могут быть изменены позднее в соответсвии с вашим сетевым окружением.

На каждом ПК, для которого вы хотите присвоить статичный IP адрес, следуйте инструкциям на страницах 11, 12 только для проверки и/или установки IP протокола. Как только он установлен, продолжите инструкции для отображения свойств протокола TCP/IP. Вместо автоматического назначения IP адреса для компьютера, DNS сервера и шлюза по умолчанию, выберите ввод информации вручную.



Примечание: IP адреса ваших ПК должны принадлежать той же подсети, что и сетевой порт RX3042H. Если вы вручную присваиваете IP для всех ваших локальных ПК, вы можете следовать инструкциям в части 5, для соответствующего изменения IP адреса маршрутизатора.

3.3 Часть 3 — Быстрая настройка RX3042H

В 3 части вы войдете в менеджер конфигурации RX3042H и сконфигурируете основные настройки вашего роутера. Для завершения этого шага вам необходимо получить необходимую информацию у вашего провайдера. Имейте в виду, здесь приведены краткие инструкции для установки и запуска RX3042H. Для подробностей вы можете обратиться к соответствующим частям руководства.

3.3.1 Настройка RX3042H

Следуйте этим инструкциям для настройки RX3042H:

12. Перед доступом к менеджеру конфигурации RX3042H, убедитесь, что HTTP прокси-сервер отключен в вашем браузере. В IE, щелкните “Tools” -> “Internet Options...” -> “Connections” tab -> “LAN settings...” и уберите галочку с “Use proxy server for your LAN ...”

13. На любом ПК, подключенном к одному из четырех сетевых портов RX3042H, откройте браузер, в адресной строке введите следующий URL и нажмите <Enter>:

http://192.168.1.1

Это встроенный IP адрес для сетевого порта RX3042H.

Появится окно входа, как показано на рис. 3.2.



Рис. 3.2 Экран входа

Если у вас проблемы с подключением к RX3042H, проверьте настроен ли ваш ПК для получения IP адреса от RX3042H. Другой способ - установите для вашего ПК IP адрес, соответствующий для сети 192.168.1.0, например 192.168.1.2.

14. Введите имя пользователя и пароль, затем нажмите "OK" для входа в менеджер конфигурации. Первый раз вы можете войти, используя значения по умолчанию:

Имя пользователя по умолчанию: admin

Пароль по умолчанию: admin



Вы можете изменить пароль в любое время (смотрите раздел 10.2 Изменение пароля и настройка системы на стр. 92).

Страница состояния системы появляется каждый раз когда вы входите в менеджер конфигурации(см. рис. 3.3).

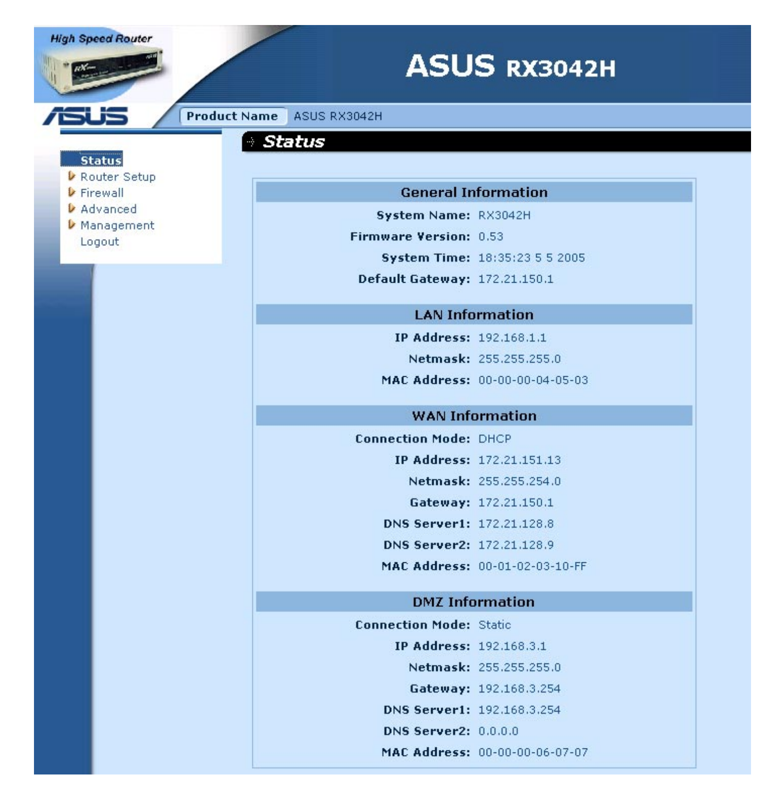


Рис. 3.3 Страница состояния системы

15. Следующие инструкции описаны в части 5 “Настройка роутера” для настройки параметров LAN и WAN для RX3042H.

После завершения основной настройки RX3042H, прочитайте следующий раздел для подключения к Интернет.

3.3.2 Проверка ваших настроек

Для проверки нужно включить любые компьютеры в вашей сети для проверки доступа к Интернет с помощью ADSL или кабельного модема.

Для проверки соединения с Интренет, откройте ваш браузер, и введите URL любого внешнего сайта (например *http://www.asus.com*). Индикатор, помеченный WAN должен быстро мигать и может гореть непрерывно когда устройство подключится к сайту. Вы также сможете просмотреть сайт через браузер.

Если индикаторы не светятся как ожидается или веб-страница не отображается, для устранения неполадок обратитесь к части 12.

3.3.3 Настройки роутера по умолчанию

Дополнительно к обработке DSL-подключения к вашему провайдеру, RX3042H может предоставить различные услуги для вашей сети. Устройство предварительно сконфигурировано для работы с домашней или небольшой офисной сетью.

В таблице 3.2 показаны некоторые наиболее важные параметры; эти и другие характеристики полностью описаны в последующих частях. Если вы знакомы с параметрами конфигурации сети, посмотрите параметры в таблице 3.2 для проверки что они соответствуют вашей сети. Если необходимо, следуйте инструкциям для их изменения. Если вы не знакомы с этими параметрами, попробуйте использовать устройство без изменения параметров или обратитесь за помощью к вашему провайдеру.

Перед изменением любых параметров, посмотрите часть 4 для общей информации об использовании программы Менеджер конфигурации. Мы настоятельно рекомендуем, чтобы вы перед изменением параметров по умолчанию, проконсультировались с вашим провайдером.

Таблица 3.2 Параметры по умолчанию

Опция	По умолчанию	Объяснение/Инструкции
DHCP (Протокол динамической конфигурации узлов)	DHCP сервер использует следущий диапазон адресов: с 192.168.1.100 по 192.168.1.200	RX3042H имеет пул IP адресов для динамического присвоения компьютерам вашей сети. Для использования этой возможности, вы должни настроить ваши компьютеры для автоматического получения IP адреса, как описано в части 2 руководства по быстрой установке. Смотрите раздел 6.1 где описывается служба DHCP.
Сетевой IP адрес	Статический IP адрес: 192.168.1.1 маска подсети: 255.255.255.0	Это сетевой IP адрес RX3042H. К LAN порту подключаются устройства вашей сети Ethernet. В большинстве случаев вам не нужно изменять этот адрес. Смотрите раздел 5.1 где описывается работа сети.

4 Использование менеджера конфигурации

RX3042H имеет программу, наэываемую менеджером конфигурации, которая предоставляет интерфейс для настройки устройства. Она позволяет вам настраивать параметры устройства для корректной работы в вашей сети. Вы можете получить доступ к нему через браузер с любого ПК, подключенного к RX3042H посредством LAN или WAN порта.

Здесь дано общее описание по использованию менеджера конфигурации.

4.1 Вход в менеджер конфигурации

Программа менеджер конфигурации установлена в RX3042H. Для доступа к программе выполните следущее:

- Подключите компьютер к LAN или WAN порту RX3042H как описано в руководстве по быстрой установке.
- Установите браузер на ваш компьютер. Программа предназначена для работы с Microsoft Internet Explorer® 6.0 или новее.

Вы можете получить доступ к программе с любого компьютера, подключенного к RX3042H посредством LAN или WAN порта. Однако инструкции, предоставленные здесь, предназначены для компьютеров, подключенных через LAN порт.

1. На компьютере, подключенном через LAN порт, откройте браузер, введите в адресную строку следущий адрес и нажмите <Enter>:

   http://192.168.1.1

   Это предопределенный IP адрес для LAN порта RX3042H. Появится окно входа, как показано на рис. 4.1.



Рис. 4.1 Окно аутентификации

2. Введите имя пользователя и пароль, затем нажмите ОК.

Используйте следущие параметры по умолчанию:

Имя пользоавателя: admin

Пароль: admin



Примечание: Вы можете изменить пароль в любое время (смотрите раздел 10.2 Изменение пароля и настройка системы на странице 92).

Страница состояния системы отображается при каждом входе в менеджер конфигурации (показана на рис. 3.3 на странице 20).

4.2 Функциональность

Типичная страница конфигурации состоит из нескольких элементов: заголовок, меню, подсказки меню навигации, конфигурация и он-лайн помощь. Вы можете нажать на любой пункт меню для раскрытия/закрытия любой группы меню или доступа к определенным страницам конфигурации. Подсказки меню навигации показывают доступ к текущей конфигурации через меню.

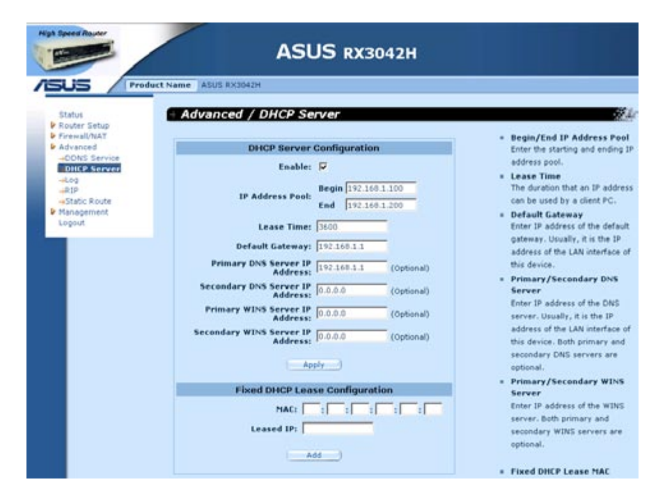


Рис. 4.2 Типичная страница менеджера конфигурации

4.2.1 Навигация в меню

- Для открытия группы связанных меню, дважды щелкните на меню или :
- Для закрытия группы связанных меню, дважды щелкните на меню или :
- Для открытия страниц конфигурации, дважды щелкните на меню или :

4.2.2 Часто используемые кнопки и иконки

В следущей таблице описаны функции для каждой кнопки или иконки, используемой в приложении.

Таблица 4.1 Часто используемые кнопки и иконки

Кнопка	Функция
Apply	Сохраняет любые изменения, сделанные на текущей странице.
Add	Добавляет существующую конфигурацию в систему, например статический маршрут или правило брандмауэра.
Modify	Изменяет существующую конфигурацию в системе, например статический маршрут или правило брандмауэра.
Reload	Обновляет текущую страницу с обновленной статистикой или параметрами.
	Выбор пункта для редактирования.
	Удаляет выбранный пункт.

4.3 Обзор конфигурации системы

Для просмотра конфигурации системы, войдите в менеджер конфигурации, или нажмите меню Status если вы уже вошли. На рис. 4.3 показана примерная информация доступная на этой странице.

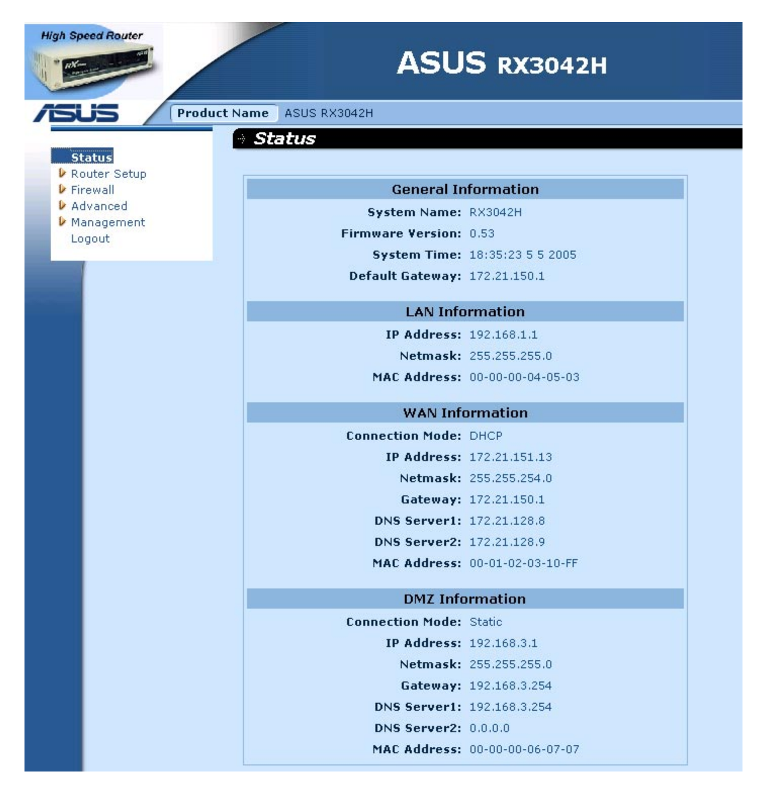


Рис. 4.3 Страница состояния системы

5 Настройка роутера

В этой части описано как сконфигурировать основные настройки вашего роутера, чтобы компьютеры в вашей сети могли взаимодействовать между собой и иметь доступ к Интернет. Настройка сети состоит из конфигурации LAN и WAN.

5.1 Конфигурация LAN

5.1.1 IP адрес

Если вы используете RX3042H с ПК в составе вашей сети, вы должны подключить вашу сеть к Ethernet-портам коммутатора. Вы должны присвоить уникальный IP адрес для каждого устройства, входящего в вашу сеть. IP адрес, идентифицирующий RX3042H в вашей сети должен иметь одинаковую подсеть с ПК вашей сети. По умолчанию IP адрес для RX3042H 192.168.1.1.



Определение: Сетевым узлом может быть любой интерфейс, подключающий устройство к сети, например сетевой порт RX3042 и сетевая карта вашего ПК. Смотрите приложение 11, где объясняются подсети.

Вы можете изменить IP адрес по умолчанию на другой, который хотите использовать в вашей сети.

5.1.2 Параметры конфигурации LAN

В таблице 5.1 описаны параметры, которые доступны для настройки IP адреса.

Таблица 5.1 Параметры конфигурации LAN

Параметр	**Описание**
Имя узла	Только для идентификации.
IP адрес	Сетевой адрес RX3042H. Этот IP адрес используется вашими компьютерами для идентификации RX3042H. Имейте в виду, что IP адрес, присвоенный вам вашим провайдером не является сетевым IP адресом. Присвоенный провайдером IP адрес идентифицирует WAN RX3042H для Интернет.
Маска подсети	Маска подсети показывает какая часть IP адреса является вашей сетью и какая определяет узел в сети. Маска по умолчанию для вашего устройства 255.255.255.0.

5.1.3 Конфигурация сетевого IP адреса

Выполните следущие шаги для изменения сетевого IP адреса.

1. Откройте страницу настройки соединения, как показано на рис. 5.1, щелкнув **Router Setup ->** меню **Connection**.

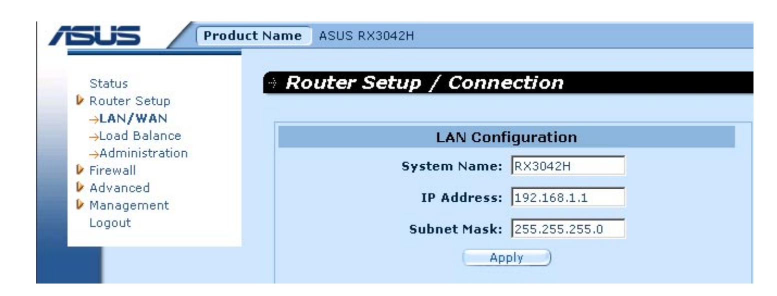


Рис. 5.1 Настройка сети - конфигурация LAN

2. (Опционально) Введите имя узла для RX3042H. Имейте в виду, что имя узла используется только для идентификации и не используется для никаких других целей.

3. Введите сетевой IP адрес и маску подсети для RX3042H.

4. Обратитесь к разделу Настройка WAN за инструкциями по настройке WAN порта, если вы еще не сделали это.

5. Нажмите "**Apply**" для сохранения параметров. Если вы используете Ethernet-соединение для текущей сессии, и изменили IP адрес или маску подсети, соединение будет разорвано.
6. Вы можете увидеть сообщение как показано ниже.

Please wait...

Changing IP or netmask ...

The page is to be redirected to: http://192.168.1.3 in 2.6 seconds.

7. Будет показана подсказка для возврата в Менеджер конфигурации по истечению времени.

5.2 Конфигурация WAN/DMZ

В этой секции описано как настроить параметры WAN/DMZ WAN-интерфейса RX3042H, который подключен к вашему провайдеру. В этом разделе вы научитесь настраивать IP адрес, DHCP и DNS сервер для WAN-интерфейса.

DMZ (демилитаризованная зона) - это узел или небольшая сеть, которая находится между надежными узлами внутренней сети, например частная корпоративная сеть и ненадежной внешней сетью, например Интернет. Обычно, в DMZ находятся устройства с интенсивным интернет-трафиком, например Web сервера, FTP сервера, SMTP (e-mail) сервера и DNS сервера. DMZ не содержит корпоративной конфиденциальной информации. В случае опасности, информация компании, не входящая в DMZ не пострадает.

Примечание: Только режим статического IP поддерживает DMZ.

5.2.1 Режим подключения WAN

RX3042H поддерживает пять режимов для WAN-соединения: со статическим IP, с динамическим IP, PPPoE (многосеансовый), PPPoE unnumbered, и PPTP. Вы можете выбрать один режим подключения WAN, требуемый вашим провайдером из выпадающего списка **Connection Mode** на странице настройки сети, как показано на рис. 5.2.

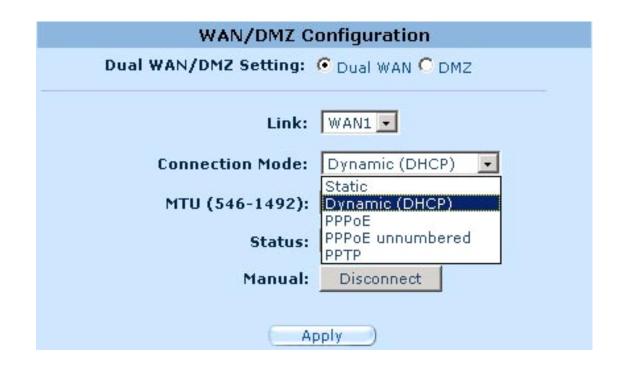


Рис. 5.2 Настройка сети - конфигурация WAN

5.2.2 PPPoE

Соединение PPPoE наиболее часто используется провайдерами ADSL.

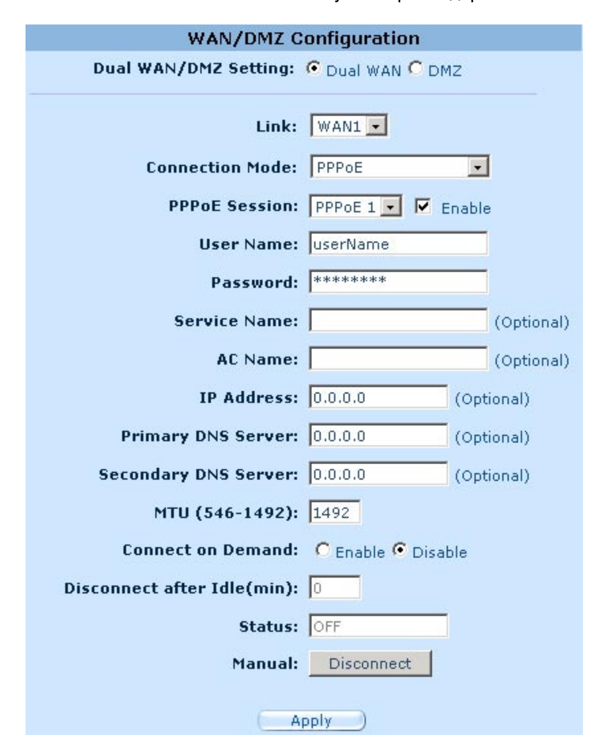


Рис. 5.3. WAN –Конфигурация PPPoE

5.2.2.1 Параметры конфигурации WAN PPPoE

В таблице 5.2 описаны параметры доступные для PPPoE-подключения.

Таблица 5.2. Параметры конфигурации WAN PPPoE

Параметр	Описание
Link	Выбор порта для настройки. Доступны опции WAN1, WAN2 или DMZ.
Connection Mode	Из списка соединений выберите PPPoE.
PPPoE Session	Выберите идентификатор сеанса PPPoE. Имейте в виду, что одновременно поддерживаются только два сеанса PPPoE.
Enable	Установите или снимите галочку для активации или деактивации этого сеанса PPPoE.
User Name and Password	Введите имя пользователя и пароль, которые вы используете для подключения к провайдеру. (Примечание: эта информация отличается от той, которую вы используете для входа в Менеджер конфигурации.)
Service Name	Введите имя сервиса, предоставляемой вашим провайдером. Имя сервиса необязательно, но может требоваться некоторыми провайдерами.
AC Name	Введите имя точки доступа, предоставляемое вашим провайдером. Имя точки доступа необязательно, но может требоваться некоторыми провайдерами.
IP Address	Если ваш провайдер предоставляет вам фиксированный IP адрес, введите его здесь.
Primary / Secondary DNS Server	IP адреса первичного и /или вторичного DNS необязательны, поскольку PPPoE обнаружит IP адреса DNS, настроенные вашим провайдером. Тем не менее, если вы хотите использовать другие серверы DNS, введите их IP адреса здесь.
MTU	Вы можете определить максимальный размер пакета. Для PPPoE, значение MTU от 546 до 1492. Значение по умолчанию 1492.

Параметр	Описание
Disconnect after idle (min.)	Введите период времени через который соединение с Интернет будет разорвано при отсутсвии трафика. Значение 0 означает никогда не разъединять. Имейте в виду, что служба SNTP, если она активна, может создавать помехи этой функции.
Connect on Demand	Щелкните Enable или Disable для включения или выключения подключения по требованию.
Status	On: Подключение PPPoE активно. Off: Нет активного PPPoE-подключения. Connecting: RX3042H пытается подключиться к вашему провайдеру, используя соединение PPPoE.
Manual Disconnect/ Connect	Щелкните кнопку Disconnect или Connect для соединения или разъединения, используя соединение PPPoE.

5.2.2.2 Настройка PPPoE для WAN

Выполните следущие инструкции для настройки параметров PPPoE:

1. Откройте страницу настройки сети, щелкнув **Router Setup ->** меню **Connection**.
2. Выберите какой WAN порт (WAN1/WAN2) настроить для PPPoE соединения.
3. Выберите **PPPoE** из выпадающего списка Connection Mode, как показано на рис. 5.3.
4. Выберите **идентификатор сеанса PPPoE** из выпадающего списка PPPoE session. К настоящему времени, каждый порт WAN поддерживает два сеанса.
5. Введите имя сервиса, если это требует ваш провайдер.
6. (Дополнительно) Введите имя AC, если это требует ваш провайдер.
7. (Дополнительно) Если провайдер предоставляет вам постоянный IP адрес, введите его в поле IP Address; иначе пропустите этот шаг.
8. (Дополнительно) Если вы хотите использовать другие серверы DNS, введите их IP адреса; иначе пропустите этот шаг.

9. (Дополнительно) Если необходимо, измените значение MTU. Если вы не знаете какое значение ввести, оставьте как есть. Для динамического IP значение MTU от 546 до 1492. Значение по умолчанию 1492.

10. Введите параметры для “**Disconnect after Idle (min)**” и “**Connect on Demand**”.

11. Нажмите "**Apply**" для сохранения параметров.

5.2.3 PPPoE Unnumbered

Некоторые ADSL-провайдеры могут предложить услугу PPPoE unnumbered. Выбер … слугу.

WAN/DMZ Configuration

Dual WAN/DMZ Setting: Dual WAN DMZ

Link: WAN1

Connection Mode: PPPoE unnumbered

Enable NAPT:

User Name: userName

Password: ********

Service Name: (Optional)

AC Name: (Optional)

IP Address: 0.0.0.0

Unnumbered network address: 0.0.0.0

Unnumbered netmask: 0.0.0.0

Primary DNS Server: 0.0.0.0 (Optional)

Secondary DNS Server: 0.0.0.0 (Optional)

MTU (546-1492): 1492

Connect on Demand: Enable Disable

Disconnect after Idle(min): 0

Status: OFF

Manual: Disconnect

Apply

Рис. 5.4. WAN – Настройка PPPoE Unnumbered

5.2.3.1 Параметры конфигурации PPPoE Unnumbered

В таблице 5.3 описаны параметры настройки соединения PPPoE Unnumbered.

Таблица 5.3. Параметры настройки PPPoE Unnumbered

Параметр	Описание
Link	Выберите порт для настройки. Доступны опции WAN1, WAN2 или DMZ.
Connection Mode	Выберите PPPoE Unnumbered из выпадающего списка соединений. Обычно, каждый сетевой интерфейс должен иметь уникальный IP адрес. Тем не менее, интерфейс unnumbered не имеет уникального IP адреса. Это означает, что когда выбрана эта опция, WAN и LAN имеют одинаковый IP адрес. Экономятся сетевые ресурсы поскольку используется меньше IP адресов и таблица маршрутизации меньше.
Enable NAPT	Установите или снимите галочку для включения или отключения NAPT для этого соединения.
User Name and Password	Введите имя пользователя и пароль, которые вы используете для подключения к вашему провайдеру. (Примечание: эта информация отличается от той, которую вы используете для входа в Менеджер конфигурации.)
Service Name	Введите имя сервиса, предоставляемой вашим провайдером. Имя сервиса необязательно, но может требоваться некоторыми провайдерами.
AC Name	Введите имя точки доступа, предоставляемое вашим провайдером. Имя точки доступа необязательно, но может требоваться некоторыми провайдерами.
IP Address	Введите IP адрес для соединения PPPoE unnumbered. Этот IP адрес должен предоставляться вашим провайдером.
Unnumbered Network Address	Введите адрес сети, предоставляемый провайдером.

Параметр	Описание
Primary / Secondary DNS Server	IP адреса первичного и /или вторичного DNS необязательны, поскольку PPPoE обнаружит IP адреса DNS, настроенные вашим провайдером. Тем не менее, если вы хотите использовать другие серверы DNS, введите их IP адреса здесь.
MTU	Вы можете определить максимальный размер пакета. Для PPPoE, значение MTU от 546 до 1492. Значение по умолчанию 1492.
Disconnect after Idle (min.)	Введите период времени через который соединение с Интернет будет разорвано при отсутсвии трафика. Значение 0 означает никогда не разъединять. Имейте в виду, что служба SNTP, если она активна, может создавать помехи этой функции.
Connect on Demand	Щелкните Enable или Disable для включения или выключения подключения по требованию.
Status	On: Подключение PPPoE активно. Off: Нет активного PPPoE-подключения. Connecting: RX3042H пытается подключиться к вашему провайдеру, используя соединение PPPoE unnumbered.
Manual Disconnect/ Connect	Щелкните кнопку Disconnect или Connect для соединения или разъединения, используя соединение PPPoE unnumbered.

5.2.3.2 Настройка PPPoE Unnumbered для WAN

Выполните следущие инструкции для настройки параметров PPPoE unnumbered:

1. Откройте страницу настройки сети, щелкнув **Router Setup ->** меню **Connection**.
2. Выберите какой WAN порт (WAN1/WAN2) настроить для соединения PPPoE unnumbered.
3. Выберите **PPPoE Unnumbered** из выпадающего списка Connection Mode как показано на рис. 5.4.
4. Установите галочку **NAPT**, если для этого соединения будет использоваться NAT.
5. Введите имя пользователя и пароль, предоставляемые вашим провайдером.
6. (Дополнительно) Введите имя AC, если это требует ваш провайдер.

7. Введите IP адрес, адрес сети unnumbered и адрес подсети unnumbered предоставляемые вашим провайдером.
8. (Дополнительно) Если вы хотите использовать другие серверы DNS, введите их IP адреса; иначе пропустите этот шаг.
9. (Дополнительно) Если необходимо, измените значение MTU. Если вы не знаете какое значение ввести, оставьте как есть. Для динамического IP значение MTU от 546 до 1492. Значение по умолчанию 1492.
10. Введите параметры для “**Disconnect after Idle (min)**” и “**Connect on Demand**”.
11. Нажмите "**Apply**" для сохранения параметров.

5.2.4 Динамический IP

Динамический IP наиболее часто используется провайдерами.

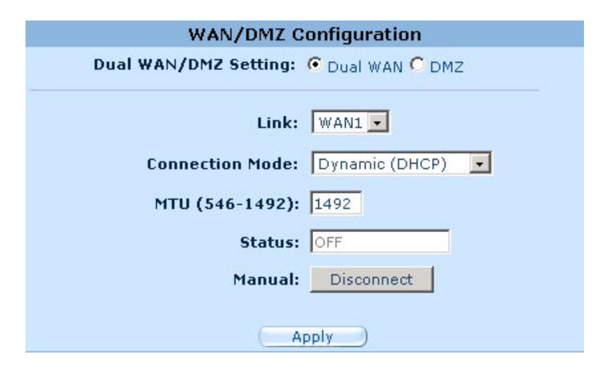


Рис. 5.5. WAN – настройка динамического IP (клиент DHCP)

5.2.4.1 Настройка динамического IP для WAN

Для настройки динамического IP выполните следущее:

1. Откройте страницу настройки сети, щелкнув **Router Setup ->** меню **Connection**.
2. Выберите какой WAN порт (WAN1/WAN2) настроить для динамического IP.
3. Выберите **Dynamic** из выпадающего списка Connection Mode, как показано на рис. 5.5. Имейте в виду, что IP для первичного и/или вторичного серверов DNS автоматически назначаются DHCP сервером

вашего провайдера.

4. (Дополнительно) Если необходимо, измените значение MTU. Если вы не знаете какое значение ввести, оставьте как есть. Для динамического IP значение MTU от 546 до 1500. Значение по умолчанию 1500.
5. Нажмите "**Apply**" для сохранения параметров.

5.2.5 Статический IP

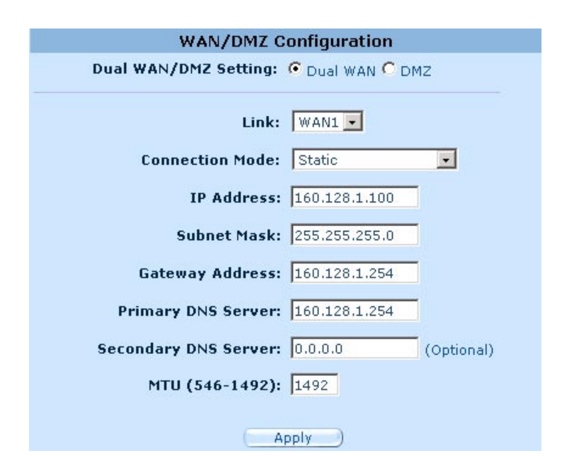


Рис. 5.6. WAN – Настройка статического IP

5.2.5.1 Параметры настройки статического IP для WAN или DMZ

В таблице 5.4 описаны параметры настройки для соединения со статическим IP.

Таблица 5.4. Параметры настройки статического IP для WAN

Параметр	Описание
Link	Выберите порт для настройки. Доступные опции WAN1/WAN2 или WAN/DMZ.
Connection Mode	Из списка соединений выберите **Static.**
IP Address	WAN/DMZ IP адрес. Пожалуйста отметьте, что WAN IP - это IP адрес, предоставляемый вашим провайдером, а DMZ IP адрес является частным IP адресом.
Subnet Mask	Маска подсети WAN/DMZ . Обычно 255.255.255.0.

Параметр	Описание
Gateway Address	IP адрес шлюза по умолчанию, предоставляемый вашим провайдером. Он должен иметь одинаковую подсеть интерфейсом WAN RX3042H.
Primary/ Secondary DNS Server	Вам нужно ввести IP адрес первичного DNS сервера. Вводить адрес вторичного DNS необязательно
MTU	Вы можете определить максимальный размер пакета. Для соединения со статическим IP диапазон MTU от 546 до 1492. По умолчанию 1492.

5.2.5.2 Настройка статического IP для WAN или DMZ

Для настройки статического IP выполните следущее:

1. Откройте страницу настройки сети, щелкнув **Router Setup ->** меню **Connection**.
2. Выберите какой WAN порт (WAN1/WAN2) или DMZ настроить для соединения.
3. Выберите **Static** из выпадающего списка Connection Mode, как показано на рис. 5.6.
4. Введите IP адрес для WAN в поле **IP Address**. Эту информацию должен предоставить ваш провайдер.
5. Введите маску подсети для WAN. Эту информацию должен предоставить ваш провайдер. Обычно это 255.255.255.0.
6. В поле **Gateway Address** введите адрес шлюза по умолчанию, предоставленный вашим провайдером.
7. Введите IP адрес первичного DNS сервера. Эту информацию должен предоставить ваш провайдер. Вводить адрес вторичного DNS необязательно.
8. (Дополнительноl) Если необходимо измените значение MTU. Если вы не знаете какое значение ввести, оставьте как есть. Для соединения с динамическим IP, диапазон MTU от 546 to 1492. По умолчанию значение 1492.
9. Нажмите "**Apply**" для сохранения параметров.

5.2.6 PPTP

Некоторые провайдеры предлагают пользователям входить, используя PPTP соединение.

5.2.6.1 Настройка параметров WAN PPTP

В таблице 5.5 описаны параметры настройки соединения PPTP.

Таблица 5.5. Параметры настройки WAN PPTP

Параметр	Описание
Link	Выберите порт для настройки. Доступны опции WAN1, WAN2 или DMZ.
Connection Mode	Выберите PPTP из выпадающего списка соединений.
WAN Interface IP	Выберите тип IP адреса для WAN – статический (ручная установка IP адреса) или динамический (получаемый от DHCP сервера).
Static	Выберите этот режим соединения, если провайдер предоставляет вам фиксированный IP адрес.
IP Address	Введите IP адрес для WAN, предоставляемый вашим провайдером.
Subnet Mask	Введите маску подсети для WAN, предоставляемую вашим провайдером.
Gateway Address	Введите IP шлюза по умолчанию для WAN, предоставляемого вашим провайдером.
Dynamic (DHCP)	Выберите этот режим соединения, если вы получаете IP адрес для WAN с провайдерского DHCP сервера.
User Name and Password	Введите имя пользователя и пароль, которые вы используете для подключения к вашему провайдеру. (Примечание: эта информация отличается от той, которую вы используете для входа в Менеджер конфигурации.)
Server IP Address	Введите IP адрес PPTP сервера, предоставляемый вашим провайдером.
MTU	Вы можете определить максимальный размер пакета. Для PPTP, значение MTU от 546 до 1460. Значение по умолчанию 1460.
MPPE	Протокол MPPE (метод шифрования данных при передаче по VPN-каналу). Установите галочку, если пакеты будут шифроваться с помощью этого протокола.
Connect on Demand	Щелкните Enable или Disable для включения или выключения подключения по требованию.

Параметр	**Описание**
Disconnect after Idle (min)	Введите период времени, через который соединение с Интернет будет разорвано при отсутсвии трафика. Значение 0 означает никогда не разъединять. Имейте в виду, что служба SNTP, если она активна, может создавать помехи этой функции.
Status	On: Подключение PPPoE активно. Off: Нет активного PPPoE-подключения. Connecting: RX3042H пытается подключиться к вашему провайдеру, используя соединение PPPoE unnumbered.
Manual Disconnect/ Connect	Щелкните кнопку Disconnect или Connect для соединения или разъединения, используя соединение PPTP.

Рис. 5.7. WAN – Настройка PPTP

5.2.6.2 Настройка PPTP для WAN

Выполните следующие инструкции для настройки параметров PPTP:

1. Откройте страницу настройки сети, щелкнув **Router Setup ->** меню **Connection**.
2. Выберите, какой WAN порт (WAN1/WAN2) настроить для соединения PPTP.
3. Выберите **PPTP** из выпадающего списка Connection Mode, как показано на рис. 5.7.
4. Выберите тип IP адреса для WAN – статический или динамический. Если ваш провайдер предоставляет фиксированный IP адрес, выберите **Static** из выпадающиго списка WAN Interface IP. Если вы не знаете, проконсультируйтесь с вашим провайдером.
5. Введите IP адрес, маску подсети и IP адрес шлюза по умолчанию для вашего WAN-соединения, если IP для WAN устанавливается вручную.
6. Введите имя пользователя и пароль, предоставляемые вашим провайдером.
7. Введите IP адрес PPTP сервера, предоставленного вашим провайдером.
8. (Дополнительноl) Если необходимо измените значение MTU. Если вы не знаете какое значение ввести, оставьте как есть. Для соединения с динамическим IP, диапазон MTU от 546 to 1460. По умолчанию значение 1460.
9. Установите галочку MPPE, если пакеты будут шифроваться с помощью этого протокола.
10. Введите параметры для “**Disconnect after Idle (min)**” и “**Connect on Demand**”.
11. Нажмите "**Apply**" для сохранения параметров.

5.3 Балансировка нагрузки и резервирование WAN

RX3042H поддерживает балансировку нагрузки и резервирование для WAN -соединения. Эта функция доступна только при выборе “Dual-WAN” на странице настройки соединений(доступна щелчком по Router Setup ->меню Connection).

Балансировка нагрузки WAN распространяется на связь через два

интерфейса WAN RX3042H, основываясь на требуемой пропускной способности интерфейсов WAN. Другая функция позволяет поддерживать работу сети при отказ одного интерфейса WAN. Если соединение на одном WAN потеряно, RX3042H будет перенаправлять трафик на действующий WAN-интерфейс.

Резервирование линий - это функция для поддержки непрерывного доступа к Интернет. Когда связь на первичном WAN будет потеряна, доступ к Интернет будет автоматически переключен на резервное WAN -соединение.

5.3.1 Настройка параметров балансировки нагрузки и резервирования линии для WAN

В таблице 5.6 описаны параметры настройки балансировки нагрузки и резервирования линии для WAN.

Таблица 5.6. Настройка параметров балансировки нагрузки и резервирования линии для WAN

Параметр	Описание
Load Balance	Выберите одну из трех доступных опций: Disable: Отключить балансировку нагрузки и резервирование линий для WAN. Auto Mode: Выберите эту опцию для включения балансировки нагрузки. Для балансировки нагрузки используется циклический алгоритм со взвешиванием (weighted round robin). Line Backup: Выберите эту опцию, если вам необходимо резервирование линий. В существующей реализации, первичное соединение всегда установлено как WAN1 и запасное всегда установлено как WAN2.
WAN1/WAN2 Bandwidth	Введите количество трафика для распределения между интерфейсами WAN. Значения должны быть в диапазоне от 0 до 100%. Например, 80% для WAN1 и 20% для WAN2 означает 80% направляется через WAN1 и 20% направляется через WAN2.
Connectivity Check	Щелкните Enable или Disable для включения или отключения этой функции. Эта функция используется для проверки состояния связи интерфейсов WAN. Если эта опция отключена, RX3042H не выполнит переключение при неудаче; это означает, что если одно из WAN-соединений оборвется, трафик, направляемый к этому соединению не будет переадресован на действующее соединение. Рекомендуется сохранить эту опцию как enabled. Тем не менее если ваш шлюз или или специфичекие сетевые устройства при проверке связи не отвечают, вам следует отключить эту функцию.

Параметр	Описание
Connectivity Check (Cont.)	В противном случае, RX3042H может некорректно определить состояние WAN и это может отразиться на балансе нагрузки или резервировании линии.
Connectivity Check Interval	Интервал времени, через который RX3042H будет проверять состояние WAN. Допустимое значение от 1 до 60 секунд.
Connectivity Check IP Address (WAN1)	Введите IP адрес сетевого устройства через которое будет проходить трафик. Это поле является дополнительным. Обычно вам не нужно вводить IP адрес здесь, если вы знаете через какое устройство должен проходить трафик.
Connectivity Check IP Address (WAN2)	Введите IP адрес сетевого устройства через которое будет проходить трафик. Это поле является дополнительным. Обычно вам не нужно вводить IP адрес здесь, если вы знаете через какое устройство должен проходить трафик.

5.3.2 Настройка балансировки нагрузки для WAN

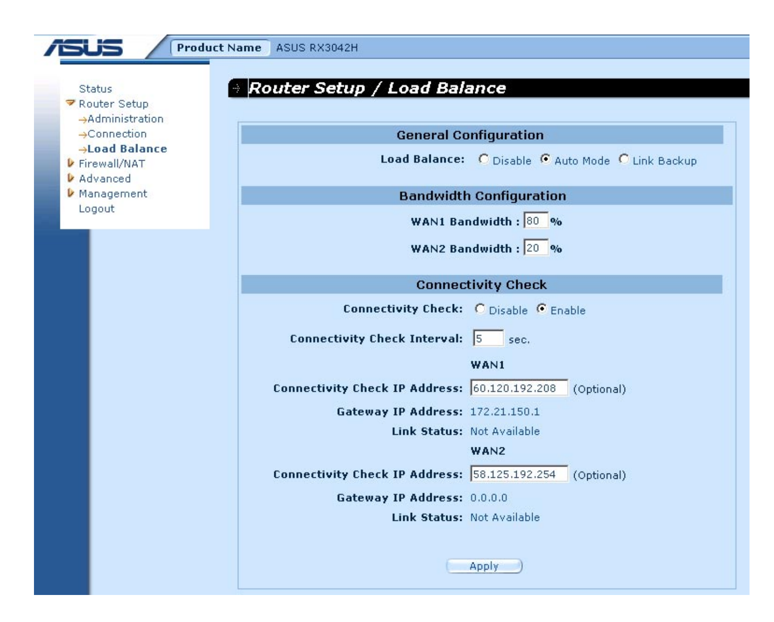


Рис. 5.8. Настройка балансировки нагрузки

Для настройки балансировки нагрузки для WAN выполните следущее:

1. Откройте страницу балансировки нагрузки, щелкнув **Router Setup ->** меню **Load Balance**.

2. В поле Load Balance выберите **Auto Mode**.

3. Введите количество трафика для распределения между интерфейсами WAN. Значения должны быть в диапазоне от 0 до 100%. Сумма обеих интерфейсов равна 100%.

4. Выберите включить или отключить проверку соединения. Если эта функция включена пожалуйста введите следущее:

a) Введите интервал для проверки соединения.

b) (Дополнительно) Введите проверяемый IP адрес для WAN1 и/или WAN2.

5. Нажмите "**Apply**" для сохранения параметров.

5.3.3 Настройка резервирования линии для WAN

Для настройки резервирования выполните следущее:

1. Откройте страницу баланс нагрузки, щелкнув **Router Setup ->** меню **Load Balance**.

2. В поле Load Balance выберите “**Line Backup**”.

3. Выберите включить или отключить проверку соединения. Если эта функция включена пожалуйста введите следущее:

a) Введите интервал для проверки соединения.

b) (Дополнительно) Введите проверяемый IP адрес для WAN1 и/или WAN2.

4. Нажмите "**Apply**" для сохранения параметров.

6 Настройка сервера DHCP

6.1 DHCP (Протокол динамической конфигурации узлов)

6.1.1 Что такое DHCP?

DHCP является протоколом, который позволяет сетевым администраторам централизовано управлять присвоением и распределением IP информации для компьютеров в сети.

Когда вы включаете DHCP в сети, вы позволяете устройству — например RX3042H — присваивать временные IP адреса для ваших компьютеров при подключении к вашей сети. Назначающее устройство называется DHCP сервером, а получающее устройство - DHCP клиентом.



Примечание: Если вы следуете инструкциям Руководства по быстрой установке, вы установили IP адрес для каждого сетевого ПК или определили получение IP адреса динамически (автоматически). Если вы выбрали динамический адрес, затем вам нужно настроить ваш(и) ПК как DHCP клиент, который будет получать IP адрес от DCHP сервера, например RX3042H.

Сервер DHCP имеет пул IP адресов и на определенное время присваивает их вашим компьютерам при подключении к сети. При необходимости он проверяет, собирает и перераспределяет адреса.

В сетях с включенным DHCP, информация IP, присваиваемая динамически предпочтительней чем статически. При каждом подключении к сети клиент DHCP может получить новый адрес из пула адресов.

6.1.2 Почему DHCP?

DHCP позволяет вам управлять IP адресами в вашей сети с помощью RX3042H. Без DHCP вам пришлось бы настраивать каждый компьютер отдельно. DHCP в основном используется в больших сетях, которые часто расширяются и обновляются.

6.1.3 Настройка сервера DHCP



Примечание: По умолчанию, сервер DHCP включен и имеет пул IP адресов с 192.168.1.100 по 192.168.1.149 (маска подсети 255.255.255.0). Для изменения диапазона адресов следуйте процедурам, описанным в этом разделе.

Сначала вы должны настроить ваш(и) ПК для получения IP адреса с сервера DHCP, затем настройте сервер DHCP:

1. Откройте страницу настройки сервера DHCP, показанную на рис. 6.1, щелкнув Advanced -> меню DHCP Server.

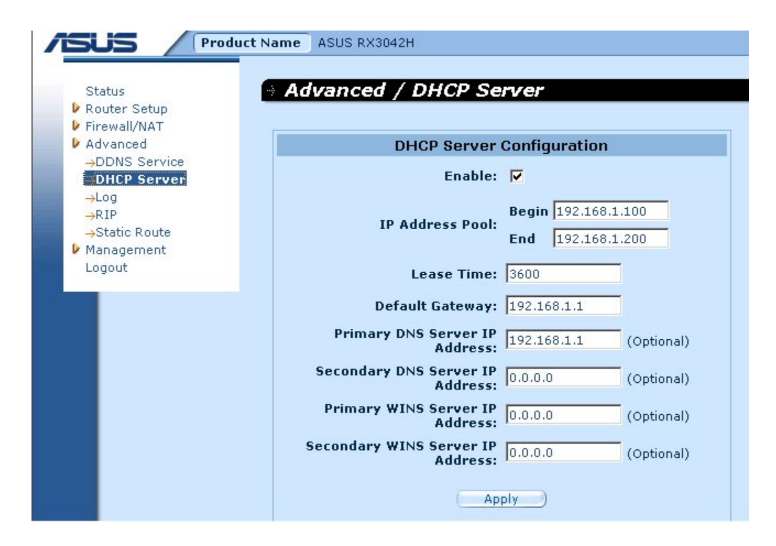


Рис. 6.1. Страница настройки сервера DHCP

2. Введите информацию для полей пула IP адресов (начало/конец), время аренды и IP адрес шлюза по умолчанию; другие, например IP адрес первичного/вторичного DNS серверов и IP адрес первичного/вторичного WINS серверов являются дополнительными. Тем не менее, рекомендуется ввести IP адрес первичного DNS сервера. Вы можете ввести IP адрес вашего сетевого DNS сервера или IP адрес DNS сервера вашего провайдера. В таблице 6.1 описаны параметры настройки DHCP сервера.

Таблица 6.1. Параметры настройки DHCP

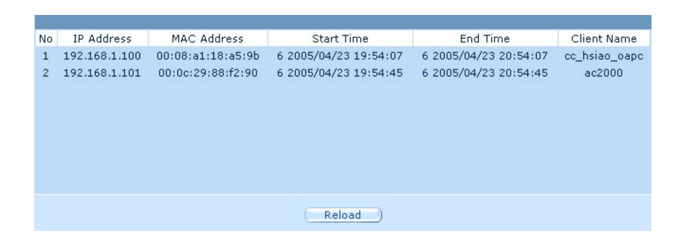
Поле	Описание
Enable	Установите или снимите галочку для включения или отключения сервера DHCP в вашей сети.
IP Address Pool Begin/End	Определите начальный и конечный адрес для пула DHCP.
Lease Time	Время в секундах, которое назначенный адрес может быть использован устройством, подключенным к сети.
Default Gateway IP Address	Адрес шлюза по умолчанию для компьютеров, которые получают IP из пула. Шлюзом по умолчанию является устройство к которому обращаются клиенты DHCP для связи с Интернет. Обычно это сетевой IP адрес RX3042H.
Primary/ Secondary DNS Server IP Address	IP адрес сервера DNS для компьютеров, которые получают IP из пула. Сервер DNS транслирует имена Интернет, которые вы пишете в вашем браузере в IP адреса. Обычно, сервер находится у вашего провайдера. Тем не менее, вы можете ввести сетевой IP адрес RX3042H, чтобы он работал как прокси DNS сервер для компьютеров в сети и пересылал DNS - запросы из локальной сети к серверу DNS и передавать результаты обратно компьютерам в локальную сеть. Имейте в виду, что оба первичный и вторичный DNS сервера необязательны.
Primary/ Secondary WINS Server IP Address (optional)	IP адрес сервера WINS используется для компьютеров, которые получают IP из пула DHCP. Вам не нужно указывать эту информацию если ваша сеть не имеет серверов WINS.

3. Нажмите **Apply** для сохранения параметров сервера DHCP.

6.1.4 Просмотр адресов, присвоенных DHCP

Когда RX3042H функционирует как сервер DHCP для вашей сети, он сохраняет записи всех адресов, выданных вашим компьютерам. Для просмотра таблицы разданных IP адрсесов, откройте страницу настройки сервера DHCP и щелкните по ссылке “Current DHCP Lease Table”, расположенной внизу страницы. Отобразится страница, аналогичная показанной на рис. 6.2.

Таблица DHCP показывает арендованные IP адреса и соответствующие MAC адреса.



No	IP Address	MAC Address	Start Time	End Time	Client Name
1	192.168.1.100	00:08:a1:18:a5:9b	6 2005/04/23 19:54:07	6 2005/04/23 20:54:07	cc_hsiao_oapc
2	192.168.1.101	00:0c:29:88:f2:90	6 2005/04/23 19:54:45	6 2005/04/23 20:54:45	ac2000

Reload

Рис. 6.2. Таблица аренды DHCP

6.1.5 Аренда фиксированного адреса DHCP

Аренда фиксированного адреса DHCP используется в ситуации когда для узла, получающего адрес с сервера DHCP необходимо установить фиксированный адрес. Сначала настройте ваш ПК для получения адреса с сервера DHCP, затем настройте сервер DHCP:

6.1.5.1 Страница настройки фиксированного адреса DHCP – (Advanced->DHCP Server)

Откройте страницу настройки фиксированного адреса DHCP, как показано на рис. 6.3, щелкнув Advanced -> меню DHCP Server.

Отметьте, что когда вы открыли страницу настройки фиксированного адреса DHCP, в нижней части будет отображен список существующих адресов, как показано на рис. 6.3.

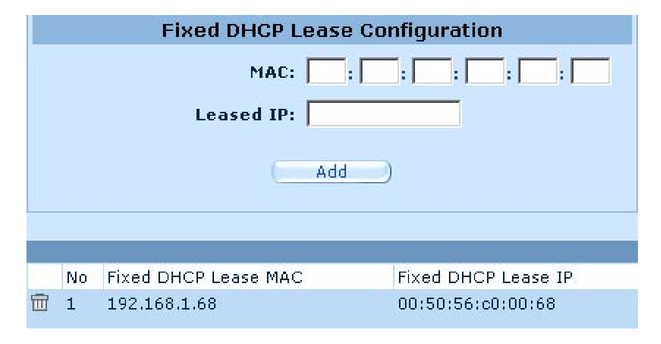


Рис 6.3. Страница настройки фиксированного адреса DHCP

6.1.5.2 Добавление фиксированного адреса DHCP

Для добавления фиксированного адреса DHCP выполните следущее:

1. Откройте страницу настройки фиксированного адреса DHCP, как показано на рис 6.3, щелкнув Advanced -> меню DHCP Server.

2. Для узла, требующего фиксированный IP адрес, введите его MAC адрес и желаемый IP адрес. В таблице 6.2 подробно описаны параметры настройки фиксированного адреса DHCP.

Таблица 6.2. Параметры настройки фиксированного адреса DHCP

Поле	**Описание**
Fixed DHCP Lease MAC	Аппаратный идентификатор устройства, которому требуется фиксированный IP адрес с сервера DHCP.
Fixed DHCP Lease IP	IP адрес, получаемый с сервера DHCP. Рекомендуется чтобы этот IP адрес был вне пула IP адресов DHCP.

3. Нажмите кнопку **Add** для добавления нового адреса DHCP.

6.1.5.3 Удаление фиксированного адреса DHCP

Для удаления фиксированного адреса DHCP, нажмите напротив фиксированного адреса DHCP.

6.1.5.4 Просмотр фиксированных адресов DHCP

Для просмотра фиксированных адресов DHCP откройте страницу настройки

фиксированных адресов DHCP, щелкнув Advanced -> меню DHCP Server

6.2 DNS

6.2.1 Что такое DNS?

Система доменных имен (DNS) транслирует интернет-адреса, которые пользователи пишут в браузере (например, “asus.com”) в эквивалентные им IP адреса, которые используют в интернет-маршрутизации.

Когда пользователь пишет адрес в браузере, ПК сначала должен послать запрос серверу DNS для получения IP адреса. Сервер DNS попытается найти этот адрес в собственной базе данных и если не найдет, то свяжется с сервром DNS следущего уровня и так далее. Когда адрес найден, он посылается обратно, запрашивающему ПК и будет использоваться для отправки IP пакетов.

6.2.2 Назначение адресов DNS

Несколько адресов DNS серверов полезно для предоставления альтернативы в случае, когда один из серверов не работает или загружен трафиком. Провайдеры обычно предоставляют первичный и вторичный сервера DNS, также могут предоставить дополнительные сервера DNS. ПК в вашей сети получают адреса серверов DNS одним из следущих способов:

- Статически: Если ваш провайдер предоставляет вам свои сервера DNS, вы можете назначить их каждому ПК в вашей сети.

- Динамически от сервера DHCP: Вы можете настроить адреса серверов DNS в сервере DHCP RX3042H и позволите серверу DHCP назначать адреса серверов DNS. Инструкции по настойке сервера DHCP смотрите раздел 6.1.3 “Настройка сервера DHCP”.

В любом случае, вы можете назначить адреса серверов DNS вашего провайдера (в ПК или на странице настройки сервера DHCP) или вы можете назначить сетевой адрес RX3042H (например, 192.168.1.1). Если вы назначили сетевой адрес устройства, устройство будет работать как ретранслятор DNS, как описано в следущем разделе.



Примечание: Если вы назначили адреса серверов DNS в ПК или в DHCP, ретранслятор DNS не используется.

6.2.3 Настройка ретранслятора DNS

Когдв вы в качестве адреса сервера DNS назначили сетевой порт устройства, роутер будет работать как “ретранслятор DNS”; так как устройство не имеет сервера DNS, оно будет пересылать запросы от компьютеров локальной сети DNS серверу провайдера. Затем будет транслировать ответ от DNS сервера обратно компьютеру в локальной сети.

При функционировании в качестве ретранслятора DNS, RX3042H должен иметь IP адреса серверов DNS. Вы можете указать адреса одним из следущих способов:

- Указать при соединении PPPoE или соединении с динамическим IP: Если RX3042H для соединения с провайдером использует PPPoE (смотрите раздел 5.2.2 PPPoE или 5.2.3 PPPoE Unnumbered) или динамический IP (смотрите раздел 5.2.4 Динамический IP), адреса первичного и вторичного серверов DNS можно узнать из протокола PPPoE. Преимущество использования этой опции в том, что вам не нужно заново конфигурировать ПК или RX3042H, если провайдер изменит адреса серверов DNS.
- Настроить RX3042H: Вы можете усказать адреса серверов DNS провайдера на странище настройки WAN как показано на рис. 5.3, рис.5.4 или рис. 5.5 или рис. 5.6.

Для настройки ретранслятора DNS выполните следущее:

1. На странице настройки DHCP введите сетевой IP адрес роутера в поле адреса сервера DNS, как показано на рис 6.1.
2. Настройте сетевые ПК для получения адресов с сервера DHCP роутера, или для каждого ПК в локальной сети в поле сервера DNS вручную введите сетевой адрес роутера.



Примечание: Адреса DNS, которые вы присвоили сетевым ПК до включения ретранслятора DNS будут применены после перезагрузки ПК. Ретранслятор DNS эффективен только когда адресом сервера DNS является сетевой IP адрес роутера.

Аналогично, если после включения ретранслятора DNS, вы указали адрес DNS (отличный от IP адреса роутера) в DHCP или статически в ПК, то этот адрес будет использоваться вместо адреса ретранслятора DNS.

7 Маршрутизация

Вы можете использовать Менеджер конфигурации для задания определенных маршрутов для вашей сети и Интернет. В этом разделе описаны основные понятия маршрутизации и предоставлены инструкции для задания статических маршрутов. Отметьте, что большинству пользователей не нужно задавать статические маршруты.

7.1 Введение в IP маршрутизацию

Основное использование маршрутизации: при получении данных, предназначенных для специфического адресата, какому следущему устройству послать эти данные? Когда вы задаете IP маршруты, вы предоставляете правила, которые RX3042H использует при принятии решений.

7.1.1 Статические маршруты

Большинству пользователей не нужно задавать статические маршруты. В небольшой домашней или офисной сети, существующие маршруты, которые установлены в шлюзе по умолчанию для компьютеров в вашей сети и для RX3042H предоставляют наиболее соответствующие маршруты для всего вашего интернет-трафика.

- Компьютерах вашей сети, шлюз по умолчанию направляет весь интернет-трафик в шлюз по умолчанию(сетевой адрес RX3042H). Компьютеры вашей сети знают свой шлюз по умолчанию поскольку вы назначили его им при изменении свойств TCP/IP, или настроили их для получения адресов от сервера DHCP. (Каждый из этих процессов описан в инструкциях Быстрого руководства по установке, часть 2.)
- Сам RX3042H настроен для направления всего уходящего интернет-трафика в шлюз провайдера. Этот шлюз автоматически назначается вашим провайдером при подключении к Интернет. (Процесс добавления маршрута по умолчанию описан в разделе 7.3.2 Добавление статических маршрутов.)

Возможно вам нужно задать статические маршруты, если у вас две или больше сетей или подсетей, или вы подключены к нескольким провайдерам, или вы подключены к удаленной корпоративной сети.

7.2 Динамическая маршрутизация с помощью RIP (протокол маршрутной информации)

RIP позволяет роутерам обмениваться информацией о маршрутах; таким образом, маршруты автоматически обновляются без участия человека. Рекомендуется чтобы вы включили RIP на странице настройки системный служб, как показано на рис. 10.1.

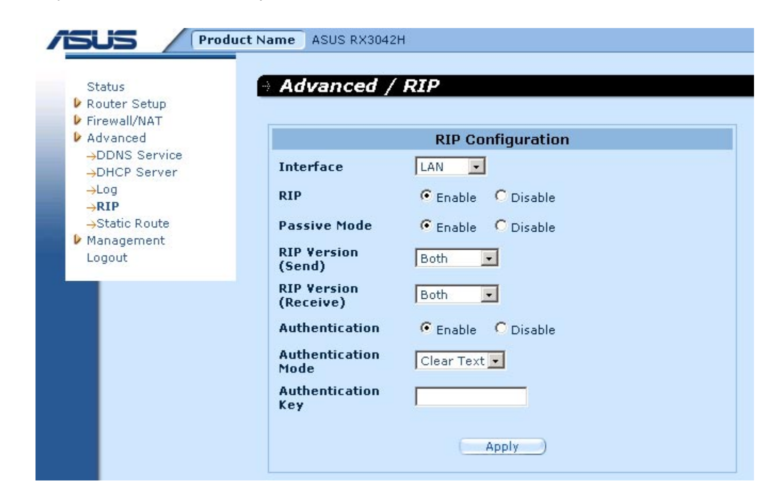


Рис. 7.1. Страница настройки RIP

7.2.1 Параметры настройки RIP

В следующей таблице описаны параметры настройки для динамической маршрутизации.

Таблица 7.1. Параметры настройки динамической маршрутизации

Поле	Описание
Interface	Выберите интерфейс, через который будет происходить обмен информацией о маршрутизации. Доступные опции LAN, WAN1, WAN2, PPPoE1, PPPoE2, PPPoE3 и PPPoE4.
RIP	Щелкните “Enable” или “Disable” для включения или отключения “RIP” на выбранном интерфейсе. Имейте в виду, что вы сначала должны включить службу RIP на странице Management / System Services.

Поле	Описание
Passive Mode	Включите этот режим, если RIP для этого интерфейса будет только принимать информацию о маршрутизации от других роутеров и не будет посылать информацию о маршрутизации другим роутерам. Отключите этот режим, если вы хотите чтобы этот интерфейс посылал и принимал информацию о маршрутизации к/от другим роутерам.
RIP Version (Send)	Выберите версию RIP для отправки информации о маршрутизации. Доступны три опции: Version 1. Version 2 и Both.
RIP Version (Receive)	Выберите версию RIP для получения информации о маршрутизации. Доступны три опции: Version 1. Version 2 и Both.
Authentication	Щелкните “Enable” или “Disable” для включения/отключения аутентификации для обмена информацией о маршрутизации. Имейте в виду, что все роутеры должны использовать одинаковый ключ аутентификации.
Authentication Mode	Выберите режим аутентификации RIP из выпадающего списка. Поддерживаются два режима - Clear Text и MD5.
Authentication Key	Введите ключ аутентификации, разделяемый всеми роутерами.

7.2.2 Настройка RIP

Выполните следущие инструкции для включения или выключения RIP:

1. На странице **System Services Configuration** (как показано на рис. 10.1), щелкните **Enable** или **Disable** в зависимости от вашего желания включить или выключить RIP.
2. Выберите интерфейс для обмена информацией из выпадающего списка (как показано на рис. 7.1).
3. Щелкните **Enable** для включения RIP для выбранного интерфейса.
4. Решите, будет ли RIP работать в пассивном режиме или нет, щелкнув **Enable** или **Disable**.
5. Выберите версию RIP для отправки и приема информации о маршрутизации. Доступные опции Version 1, Version 2 и Both.

6. Выберите, требуется ли аутентификация, щелкнув **Enable** или **Disable**.
7. (Дополнительно) Если аутентификация включена, вы также должны выбрать режим аутентификации и ключ.
8. Нажмите **Apply** для сохранения параметров.

7.3 Статическая маршрутизация

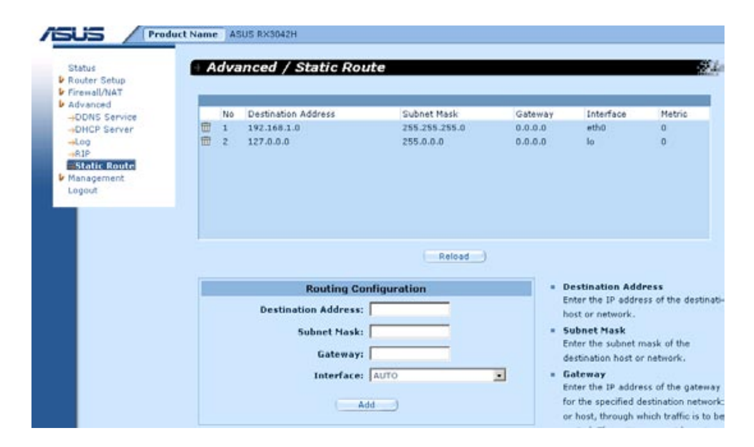


Рис. 7.2. Страница настройки статической маршрутизации

7.3.1 Параметры статической маршрутизации

В следущей таблице описаны параметры настройки для статической маршрутизации.

Таблица 7.2. Параметры настройки статической маршрутизации

Поле	Описание
Destination Address	Определите IP адрес назначения компьютера или целой сети. Он также может быть определен как все нули, показывая, что этот маршрут следует использовать для всех адресатов, для которых никакой другой маршрут не определен (это маршрут шлюза по умолчанию). Отметьте, что IP адресата должен быть идентификатором сети. Маршрут по умолчанию использует IP адресата 0.0.0.0. Смотрите приложение 11 где объясняются идентификаторы сетей.

Поле	Описание
Subnet Mask	Указывает какая часть адреса является идентификатром сети, а какая идентификатором узла. Смотрите приложение 11, где объясняются маски сети. Маршрут по умолчанию использует 0.0.0.0 для маски подсети.
Gateway	IP адрес шлюза
Interface	Доступные опции AUTO, Eth0 (LAN), Eth1 (WAN), PPPoE:0 (unnumbered), PPPoE:1 (1st PPPoE session), PPPoE:2 (2nd PPPoE session). Эти опции выбираются из выпадающего меню. Если выбрано AUTO, роутер автоматически выберет интерфейс для маршрутизации пакетов, основываясь на IP адресе шлюза.

7.3.2 Добавление статических маршрутов

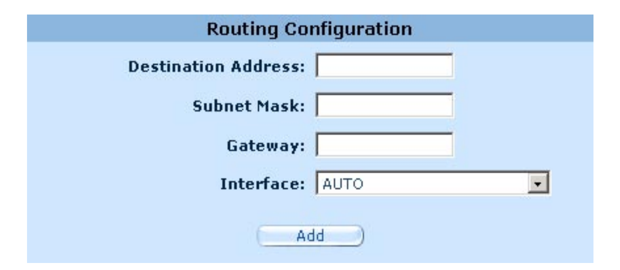


Рис. 7.3. Настройка статичекой маршрутизации

Для добавления маршрута в таблицу выполните следущие инструкции.

1. Откройте страницу **Static Route**, щелкнув **Advanced ->** меню **Static Route**.

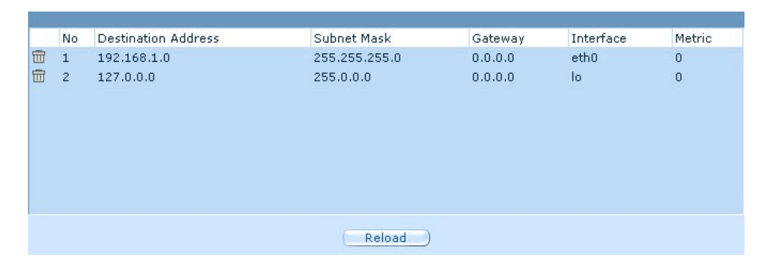
2. В соответвствующие поля введите информацию о маршруте, например IP адресата, маска подсети адресата, IP шлюза и интерфейс.

   Описание этих полей смотрите в таблице 7.2. Параметры настройки статической маршрутизации.

   Для создания маршрута, который определяет шлюз по умолчанию, введите 0.0.0.0 в следущие поля: IP адресата и маска подсети.

3. Нажмите **Add** для добавления нового маршрута.

7.3.3 Удаление статических маршрутов



	No	Destination Address	Subnet Mask	Gateway	Interface	Metric
	1	192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
	2	127.0.0.0	255.0.0.0	0.0.0.0	lo	0

Рис. 7.4. Образец таблицы маршрутизации

Для удаления статического маршрута из таблицы выполните следущие инструкции.

1. Откройте страницу настройки статических маршрутов, щелкнув **Advanced ->** меню **Static Route**.

2. Щелкните на иконке для удаления маршрута из таблицы маршрутизации.



ВНИМАНИЕ Не удаляйте маршрут по умолчанию если не знаете что делаете. Удаление маршрута по умолчанию сделает Интернет недоступным.

7.3.4 Просмотр таблицы статических маршрутов

Все IP-совместимые компьютеры и роутеры поддерживают таблицу IP адресов, которая обычно доступна их пользователям. Для каждого адресата, в таблице перечислены IP адреса первого шлюза. Эта таблица известна как таблица маршрутизации устройства.

Для просмотра таблицы марошрутизации RX3042H, щелкните **Advanced ->**меню **Static Route**. Таблица маршрутизации показана вверху страницы страницы настройки статической маршрутизации, на рис. 7.2:

В таблице маршрутизации показана строка для каждого существующего маршрута, содержащая IP сети адресата, маску подсети адресата и IP адрес шлюза, пересылающего трафик.

8 Настройка DDNS

Динамический DNS (DDNS) является службой, предоставляющей компьютерам одинаковое доменное имя, даже при смене IP адреса (во время перезагрузки или при получении IP адреса от DHCP провайдера). RX3042H подключается к службе DDNS провайдера каждый раз при смене IP адреса для WAN. Это поддерживает установку веб-служб, типа Web сервера, FTP сервера, используя доменное имя вместо IP адреса. DDNS поддерживает для клиентов DDNS следующие функции:

- Обновление записей DNS (дополнение)
- Принудительное обновление DNS

Клиент HTTP DDNS

Клиент HTTP DDNS использует механизм, предоставляемый DDNS, обеспечивающий динамическое обновление записей DNS. В этом случае служба обновляет записи DNS в DNS. RX3042H использует HTTP для запуска этого обновления. RX3042H поддерживает HTTP DDNS обновление с помощью следующих служб:

- www.dyndns.org

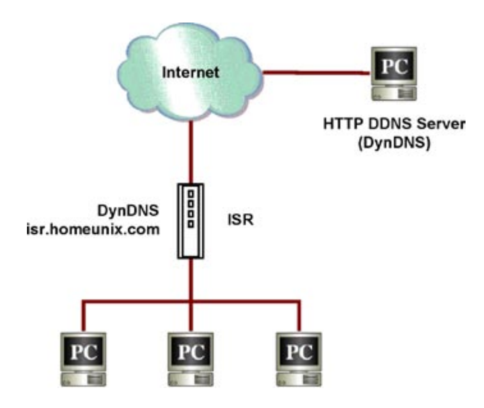


Рис. 8.1. Сетевая диаграмма для HTTP DDNS

Всякий раз, когда IP адрес, настроенный в DDNS изменяется, обновление DDNS посылают указанной службе DDNS. RX3042H должен быть настроен с именем пользователя и паролем, которые получены от вашей службы DDNS.

8.1 Настройка параметров DDNS

В таблице 8.1 описаны параметры настройки службы DDNS.

Таблица 8.1. Параметры настройки DDNS

Поле	Описание
Interface	Выберите интерфейс, который используется службой DDNS.
Status	Показывает состояние DDNS.
Enable DDNS	Поставьте галочку для включения службы DDNS.
Domain Name	В это поле введите зарегистрированное доменное имя. Например, Если имя узла вашего RX3042H “host1” и доменное имя “yourdomain.com”, полное доменное имя (FQDN) будет “host1.yourdomain.com”.
Username	Введите имя пользователя, предоставленное службой DDNS.
Password	Введите пароль, предоставленный службой DDNS.

8.2 Настройка клиента HTTP DDNS

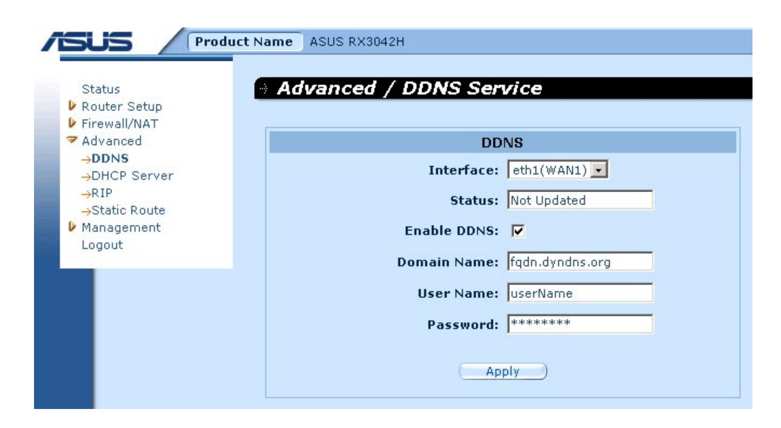


Рис. 8.2. Страница настройки HTTP DDNS

Для настройки HTTP DDNS выполните следующие инструкции:

1. Во-первых вам нужно зарегистрировать доменное имя в службе DDNS, dyndns. Если вы не сделали это, пожалуйста посетите www.dyndns.org.
2. Откройте страницу настройки DDNS, щелкнув **Advanced ->** меню **DDNS Service**.
3. Выберите интерфейс, который будет использоваться службой DDNS.
4. Установите галочку **Enable DDNS** для включения службы DDNS.
5. В поле **Domain Name** введите зарегистрированное доменное имя.
6. Введите имя пользователя и пароль, предоставленные службой DDNS.
7. Нажмите кнопку **Apply** для отправки запроса обновления DNS службе DDNS. Отметьте, что запрос обновления DNS также будет отправляться службе DDNS автоматически при изменении состояния интерфейса WAN.

9 Настройка брандмауэра и NAT

RX3042H предоставляет функции встроенного брандмауэра/NAT, позволяющие вам защитить систему от DoS-атак и других типов злонамеренного доступа к вашей сети одновременно предоставляя доступ в Интернет. Вы также можете решить как контролировать предпринятые атаки и кого следует автоматически извещать об этом.

В этой части описано как создавать/изменять/удалять ACL (список контроля доступа) для управления данными, проходящими через вашу сеть. Вы можете использовать страницу настройки брандмауэра для:

• Общей настройки брандмауэра и параметров DoS

• Создания, измения, удаления и просмотра правил ACL.

Примечание: Когда вы определяете правило ACL, вы указываете RX3042H проверять каждый пакет на соответствие его критериям, установленным в правиле. Критерием может быть сеть или протокол, направление (например, из локальной сети в Интернет или наоборот), IP адрес посылающего компьютера, IP адрес назначения и другие параметры.

Если пакет соответствует критериям, пакет либо принимается (пересывается по назначению) либо отбрасывается, в зависимости от действия, установленного в правиле.

9.1 Обзор брандмауэра

9.1.1 Проверка содержимого пакетов

Проверка содержимого пакетов RX3042H построена на таблице, которая используется для сохранения состояния соединений всех пакетов, проходящих через брандмауэр. Брандмауэр откроет “канал передачи”, позволяя пакетам проходить, если состояние пакета будет соответствовать установленному соединению. В противном случае пакет будет отброшен. Этот “канал передачи” будет закрыт, когда соединение будет завершено. Проверка содержимого пакетов включена по умолчанию при работе брандмауэра. Пожалуйста смотрите раздел 9.3.1 “Брандмауэр” для включения или отключения брандмауэра RX3042H.

9.1.2 Защита от DoS (отказ в обслуживании)

Защита от DoS-атак и проверка содержимого пакетов обеспечивают первую линию защиты вашей сети. Для защиты вашей сети настройка не требуется если в RX3042H включен брандмауэр. Брандмауэр включен по умолчанию на заводе. Пожалуйста смотрите раздел 9.3.1 “Брандмауэр” для включения или отключения брандмауэра RX3042H.

9.1.3 Брандмауэр и список контроля доступа (ACL)

9.1.3.1 Приоритет правил ACL

Все правила ACL имеют назначенный идентификатор, чем меньше идентификатор, тем выше приоритет. Брандмауэр проверяет трафик, просматривая заголовки пакетов и, основываясь на правилах таблицы ACL отбрасывает их или передает дальше. Отметьте, что проверка правил ACL начинается с правила с наименьшим идентификатором и продолжается пока не найдено соответствие или проверены все правила ACL. Если соответствия не найдено, пакет отбрасывается; в противном случае, передача или отбрасывание пакета основывается на действии, определенном в соответствующем правиле ACL.

9.1.3.2 Прослеживание подключения

Механизм проверки содержимого пакетов в брандмауэре сохраняет информацию о состоянии или процессе сетевого соединения. Храня информацию о каждом подключении в таблице, RX3042H может быстро определить, принадлежит ли пакет уже установленному подключению. Если да, он пересылается через брандмауэр без сопоставления с правилами ACL.

Например, правило ACL позволяет проходить ICMP пакетам с 192.168.1.1 к 192.168.2.1. Когда 192.168.1.1 посылает ICMP запрос (например команда ping) к 192.168.2.1, 192.168.2.1 пошлет ICMP ответ к 192.168.1.1. Вам не нужно в RX3042H создавать другое правило ACL, потому что механизм проверки пакетов помнит состояние подключения и разрешит ICMP ответу пройти через брандмауэр.

9.1.4 Правила ACL по умолчанию

RX3042H поддерживает два типа правил:

- Правила ACL: для управления доступом к компьютерам в локальной сети и DMZ и для управления доступом к внешним сетям для узлов в

локальной сети и DMZ.

- Собственные правила доступа: для управления доступом к самому RX3042H.

Правила доступа по умолчанию

- Весь трафик с внешних узлов к узлам сети и DMZ отвергается.
- Весь трафик из локальной сети передается во внешнюю сеть, используя NAT.



ВНИМАНИЕ: Нет необходимости удалять правило по умолчанию из таблицы правил ACL! Лучше создать правило ACL с более высоким приоритетом для отмены правила по умолчанию.

9.2 Обзор NAT

Трансляция сетевых адресов позволяет использовать одно устройство, типа RX3042H, которое будет действовоть как посредник между Интернет (общественная сеть) и локальной (частной) сетью. Это означает, что IP адрес NAT может представлять целую группу компьютеров для любого объекта за пределами сети. Преобразование сетевых адресов (NAT)- это механизм для сохранения зарегистроированных IP адресов в больших сетях и упрощение управления IP адресами. Из-за трансляции IP адресов, NAT также скрывает сетевую структуру от посторанних глаз и обеспечивает определенный уровень безопасности локальной сети.

NAT поддерживает следущие режимы: статическую NAT, динамическую NAT, NAPT, реверсивную статическую NAT и реверсивную NAPT.

9.2.1 NAPT (трансляция сетевых адресов и портов) или PAT (трансляция портов)

Также называется IP Masquerading, эта функция отображает любые внутренние узлы к одному интернет-адресу. Отображение имеет пул сетевых портов, которые используются для трансляции. Каждому пакету назначается общий интернет-адрес и неиспользуемый номер порта из пула сетевых портов. На рис. 9.1 показано, что все узлы в локальной сети получают доступ к Интренет через один общий IP адрес и различные номера портов из свободного пула сетевых портов.

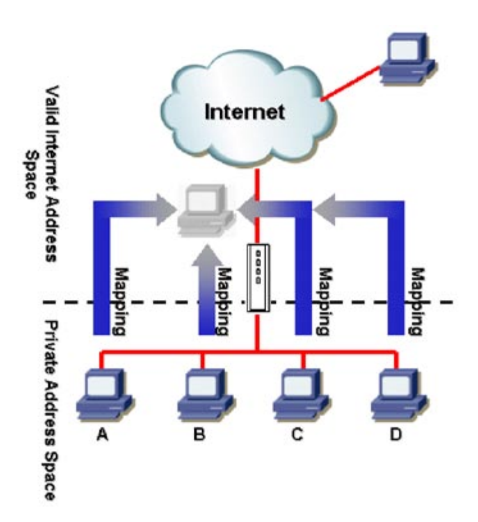


Рис. 9.1 NAPT – предоставляет внутренним ПК один общий IP адрес

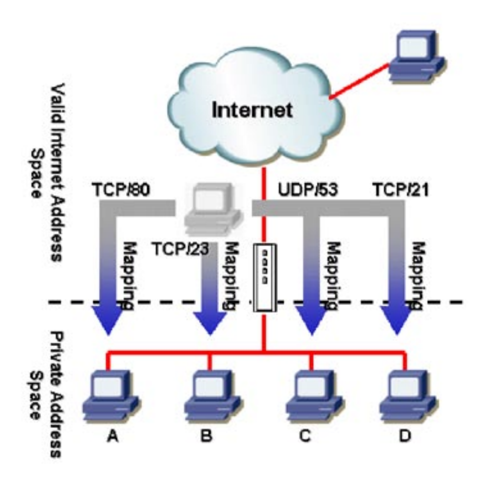


Рис. 9.2 Реверсивная NAPT – поступающие пакеты для внутеренних узлов основываются на протоколе, номере порта или IP адресе

9.2.2 Реверсивная NAPT / виртуальный сервер

Реверсивная NAPT также называемая входящим отображением, отображением портов или виртуальным сервером. Любой пакет, приходящий в RX3042H может быть передан внутреннему узлу, основываясь на протоколе, номере порта и/или IP адресе, определенных в правилах ACL. Это полезно когда много служб работают на различных внутренних узлах. На рис. 9.2 показан веб-сервер (TCP/80) на PC A, телнет-сервер (TCP/23) на PC B, DNS сервер (UDP/53) на PC C и FTP сервер (TCP/21) на PC D. Это означает, что входящий трафик этих четырех служб будет направлен к соответствующим узлам этих служб.

9.3 Параметры брандмауэра – (Firewall/NAT ->Settings)

9.3.1 Параметры брандмауэра

В таблице 9.1 l перечислены параметры брандмауэра.

Таблица 9.1. Параметры брандмауэра

Поле	Описание
DoS Check	Установите или снимите галочку для включения или отключения проверки DoS-атак. Когда опция отключена, следущие службы будут отключены: • Проверка содержимого пакетов • Проверка DoS-атак
Default NAT	
Log Port Probing	Если эта опция включена, попытки подключения к закрытым портам будут регистрироваться.
Stealth Mode	Если включена, RX3042H не будет реагировать на попытки подключения к закрытым TCP/UDP портам.

Для настройки параметров брандмауэра выполните следущее:

1. Откройте страницу настройки брандмауэра как показано на рис. 9.3, щелкнув **Firewall/NAT ->** меню **Settings**.
2. Включите или отключите опции брандмауэра.
3. Нажмите **Apply** для сохранения параметров.

9.3.2 Настройка DoS

RX3042H имеет механизм защиты от атак, который защищает внутренние сети от DoS-атак типа SYN flooding, IP smurfing, LAND и т.п. Он может отбрасывать перенаправляемые ICMP и IP пакеты с неизвестным адресом. Например, брандмауэр RX3042H обеспечивает защиту от “WinNuke”, широко используемой в Интернет программы для удаленного разрушения систем Windows. Брандмауэр RX3042H также предоставляет защиту от различных интренет-атак типа IP Spoofing, Ping of Death, Land Attack и Reassembly attacks. Полный список DoS-атак, обнаруживаемых RX3042H, пожалуйста смотрите в таблице 2.1.

9.3.2.1 Параметры настройки защиты от DoS-атак

В таблице 9.2 предоставлено объяснение DoS-атак. Вы можете установить галочку или снять ее для включения или выключения защиты для каждого типа DoS-атак.

Таблица 9.2. Определение DoS-атак

Поле	Описание
IP Source Route	Для выведения из строя системы злоумышленник использует “маршрутизацию источника”.
IP Spoofing	Spoofing -это создание TCP/IP пакетов, используя чей-нибудь IP адрес. IP spoofing- это часть сетевых атак, которым не нужно видеть ответы.
Land	Злоумышленник посылает пакеты в систему с одинаковым адресом источника и места назначения, являющимся IP адресом атакуемого компьютера. Это приводит к тому, что компьютер-жертва пытается установить соединение сам с собой, в результате чего сильно возрастает загрузка процессора и может произойти "подвисание" или перезагрузка
Ping of Death	Нападение выполняется путем посылки ping пакета, размер которого превышает 64Кб. Этот пакет делится на фрагменты и получающий узел при попытке собрать этот этот большой пакет обычно перезагружается.
Smurf	smurf-атаки используют широковещательный адрес IP-сети в качестве адреса назначения. В качестве IP адреса источника используется поддельный IP адрес. Злоумышленник посылает пакеты ICMP echo requests , используя в качестве IP адреса источника адрес жертвы. Получив пакет с запросом, все узлы вашей сети вышлют множество ответных пакетов на адрес жертвы. Таким образом ваша локальная сеть становится посредником в smurf-атаке.

Поле	Описание
SYN/ ICMP/ UDP Flooding	Включите или отключите эту опцию для регистрации SYN/ ICMP/UDP flooding-атак. Эти атаки основаны на отпавке множества TCP SYN/ICMP/UDP пакетов за короткий период. RX3042H не будет отбрасывать наводняющие пакеты чтобы не затронуть нормальный трафик.
TCP XMAS/ NULL/ FIN Scan	Хакер может сканировать вашу систему, посылая специально форматированные пакеты для просмотра доступных служб. Иногда это подготовка для будущих атак или поиск в вашей системе служб, которые восприимчивы к атакам. XMAS scan: TCP пакет имеет последовательность нулей и установленные биты FIN, URG и PUSH . NULL scan: TCP пакет имеет последовательность нулей и все служебные биты установлены в нуль. FIN scan: Хакер сканирует систему, используя “stealth” метод. Цель хакера узнать можно ли подключиться к системе без реального соединения, используя “FIN” сканирование. Все способы приводят к ошибкам, но некоторые системы отвечают с различными ошибками в зависимости от доступности или недоступности службы.
Re-assembly	В teardrop-атаке, злоумышленник помещает запутанное значение смещения в следующий или последующий фрагмент. Если принимающая система не готова к этой ситуации, это может привести к перезагрузке системы.
WinNUKE	Включите или отключите эту опцию для защиты от Winnuke -атак. Некоторые старые версии ОС Windows уязвимы для этой атаки. Если компьютеры в локальной сети не защищены последними патчами, вам следует включить эту защиту, установив галочку.

9.3.2.2 Настройка фильтра для DoS-атак

Для настройки параметров фильтра для DoS-атак выполните следующее:

1. Откройте страницу настройки брандмауэра как показано на рис. 9.3, щелкнув **Firewall** -> меню **Settings**.
2. Установите или снимите галочку индивидуально для каждого типа защиты от DoS-атак.
3. Нажмит**е Appl**y для сохранения параметров.

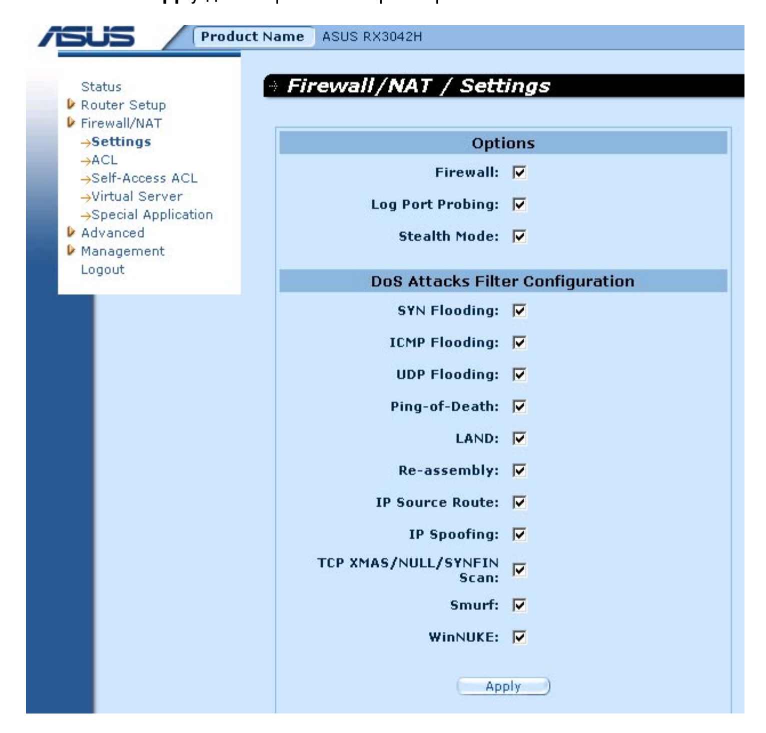


Рис. 9.3. Страница настройки брандмауэра

9.4 Параметры настройки правил ACL

9.4.1 Параметры настройк правил ACL

В таблице 9.3 описаны параметры брандмауэра для входящих, выходящих и собственных правил ACL.

Таблица 9.3. Параметры настройки правил ACL

Поле	Описание
Traffic Direction – Выберите доступную опцию из выпадающего списка для настройки ACL. Для конфигурации dual-WAN доступны две опции – LAN ->WAN and WAN ->LAN. Для конфигурации WAN + DMZ доступны шесть орций – LAN ->WAN, WAN ->LAN, LAN ->DMZ, DMZ->LAN, WAN ->DMZ и DMZ ->WAN.	
ID	
Add New	Нажмите на эту опцию для добавления нового правила ACL.
Rule Number	Выберите из списка правило для изменения параметров.
Move to Эта опция позволяет вам установить приоритет для этого правила. Брандмауэр RX3042H работает с пакетами, основываясь на приоритете. Установите приоритет, установив номер для этой позиции в списке правил:	
1 (первый)	Этот номер обозначает высший приоритет.
Другие номера	Выберите другие номера для указания приоритета.
Log Установите галочку для включения регистрации для этого правила ACL; в противном случае оставьте его пустым.	
Action	
Allow	Выберите эту опцию для разрешения . Это правило будет пропускать пакеты, проходящие через брандмауер.
Deny	Выберите эту опцию для запрещения. Это правило будет отбрасывать пакеты, проходящие через брандмауер.
Route to – сохраните параметро “AUTO” если пакеты не направлены к определенному интерфейсу. Доступны следущие опции: AUTO, eth1 (WAN1), eth2 (WAN2), PPP1 (WAN1-unnumbered), PPP1 (WAN2-unnumbered), PPP3 (WAN1-PPPoE1), PPP4 (WAN1-PPPoE2), PPP5 (WAN2-PPPoE1), PPP6 (WAN2-PPPoE2). Если интерфейс WAN установлен в режим DMZ, доступны только AUTO, eth1, PPP1/3/4. Эти опции выбираются из выпадающего меню. Если выбрано AUTO, роутер будет пересылать пакеты, основываясь на информации в таблице маршрутизации.	

Поле	Описание
NAT	
None	Выберите эту опцию, если вы не собираетесь исполььзовать NAT в этом правиле ACL.
IP Address	Выберите эту опцию для определения IP адреса, который вы хотите использовать как IP адрес источника для выходящего трафика.
Auto	RX3042H автоматически использует IP адрес интрфейса, который передает трафик как исходный IP адрес. Рекомендуется чтобы вы выбрали эту опцию, если NAT будет использоваться для выходящего трафика
Source Эта опция позволяет установить исходную сеть, к которой относится это правило. Используйте выпадающий список для выбора следующих опций:	
Any	Эта опция позволяет вам применить это правило ко всем компьютерам в исходной сети, например для входящего интернет-трафика или для исходящего трафика всех компьютеров в локальной сети.
IP Address	Эта опция позволяет вам определить IP адрес, для которого применяется это правило
Network Address	Определите соответствующий сетевой адрес
Subnet	Эта опция позволяет вам включать все компьютеры, подключенные к IP подсети. Когда эта опция выбрана, становятся доступны следущие поля:
Поле	**Описание**
Address	Введите соответствующий IP адрес.
Mask	Введите соответствующую маску подсети.
MAC Address	Эта опция позволяет вам определить MAC адрес, к которому применяется это правило.
MAC	Введите желаемый MAC адрес.
Destination Эта опция позволяет вам установить сеть назначения, к которой применяется это правило. Используйте выпадающий список для выбора одной из следущих опций:	
Any	Эта опция позволяет вам применить это правило ко всем компьютерам в локальной сети для входящего или исходящего трафика.

IP Address, Subnet	Выберите любую из этих опций, подробности описаны выше в разделе Source IP.
Service Выберите службу из выпадающего списка, к которой применяется это правило. Если желаемой службы нет в списке, нажмите кнопку Edit для создания новой службы.	
Time Выберите время для применения этого правила.	
Enable	Установите галочку, если вы хотите задействовать правило ACL в определенное время. В противном случае правило активно все время
Date and Time	Выберите желаемую дату и время для этого правила ACL.

Таблица 9.4. Параметры настройки служб

Поле	Описание
Service Name Введите имя, идентифицирующее новую службу.	
Protocol Выберите протокол из выпадающего списка. Доступны следущие опции All, TCP, UDP, ICMP, IGMP, AH ESP и TCP/UDP.	
Port Эта опция позволяет вам указать номер(а) порта, используемого устройства. Используйте выпадающий список для выбора одной из следущих опций:	
Any	Выберите эту опцию, если служба используется для определения произвольного приложения.
Single	Выберите эту опцию, если служба использует специфический номер порта.
Port Number	Введите номер порта
Range	Выберите эту опцию, если служба использует диапазон портов. Когда эта опция выбрана, становятся доступными следущие поля.
Start Port	Введите начало диапазона портов
End Port	Введите окончание диапазона портов

Поле	Описание
Эта опция позволяет вам выбрать тип сообщения ICMP. Поддерживаются следущие типы сообщений ICMP: • Любой (по умолчанию) • 0: Эхо-ответ • 1: Тип 1 • 2: Тип 2 • 3: Отключение источника при переполнении очереди • 4: Src quench: source quench • 5: Переадресовать • 6: Тип 6 • 7: Тип 7 • 8: Эхо запроса • 9: Объявление маршрутизатора • 10: Запрос маршрутизатора • 11: Время жизни истекло • 12: Проблема с параметрами • 13: Запрос временной метки • 14: Временная метка-отклик • 15: Запрос информации • 16: Информационный отклик • 17: Запрос адресной маски • 18: Отклик на запрос адресной маски	

9.5 Настройка правил ACL – (Firewall ->ACL)

Создание правил ACL на странице настройки ACL показано на рис. 9.4, вы можете задать контроль (разрешить или отбросить) для обеих надежной и ненадежной сетей.

Опции на странице настройки позволяют вам следущее:

- Добавление правила, и настройка его параметров
- Изменение существующих правил
- Удаление существующих правил
- Просмотр правил ACL

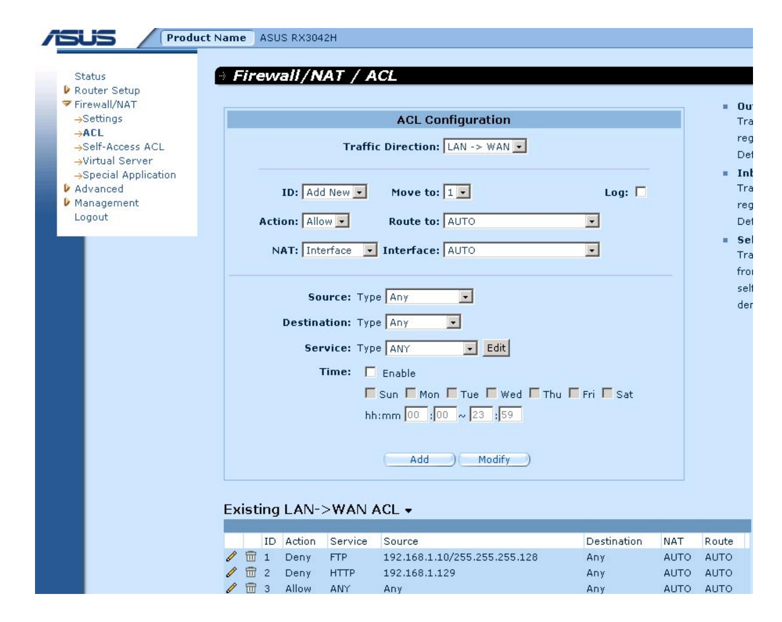


Рис. 9.4. Страница настройки ACL

9.5.1 Добавление правила ACL

Для добавления правила ACL, выполните следущее:

1. Откройте страницу натройки правил ACL, как показано на рис. 9.4, щелкнув **Firewall ->** меню **ACL** .
2. Выберите опцию из выпадающего списка **Traffic Direction**. Например, если вы хотите соосдать ACL для фильтрации трафика, порожденного локальной сетью и предназначенного для WAN, выберите опцию **LAN ->WAN**.
3. Выберите **Add New** из выпадающего списка “ID”.
4. Установите желаемое действие (разрешить или отбросить) из выпадающего списка **Action**.
5. Выберите из выпадающего списка **Route To** , если вы предполагаете направлять трафик в определенный интерфейс. Выберите AUTO для маршрутизации трафика автоматически.
6. Выберите тип NAT и введите необходимую информацию для выбранного типа NAT.

7. Сделайте изменения для любого или всех следущих полей: source/ destination IP, service, time и log. Для объяснения этих полей пожалуйста смотрите таблицу 9.3.

8. Присвойте приоритет для этого правила, выбрав номер из выпадающего списка **Move to**. Отметьте, что номер указывает приоритет правила, 1 является наивысшим приоритетом. Правила с высоким приоритетом в брандмауэре проверяются перед правилами с низким приоритетом.

9. Нажмите кнопку **Add** для создания нового правила ACL. Новое правило ACL будет отображено в таблице контроля доступа внизу страницы настройки ACL.

На рис. 9.5 показано как создать правило для блокирования HTTP трафика, порожденного узлом с IP адресом 192.168.1.129.

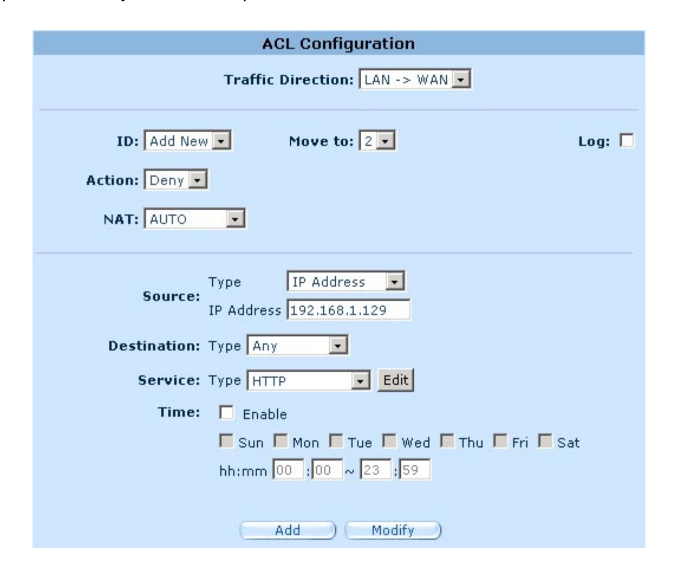
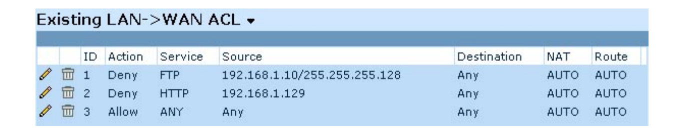


Рис. 9.5. Пример настройки ACL



Existing LAN->WAN ACL

		ID	Action	Service	Source	Destination	NAT	Route
		1	Deny	FTP	192.168.1.10/255.255.255.128	Any	AUTO	AUTO
		2	Deny	HTTP	192.168.1.129	Any	AUTO	AUTO
		3	Allow	ANY	Any	Any	AUTO	AUTO

Рис. 9.6. Образец таблицы ACL

9.5.2 Модификация правил ACL

Для модификации правила ACL выполните следующие инструкции:

1. Откройте страницу настройки правил ACL, щелкнув **Firewall/NAT ->** меню **ACL**.
2. Нажмите иконку правила для его модификации или выберите номер правила из выпадающего списка **ID**.
3. Сделайте желаемые изменения для любого или всех следущих полей: action, source/destination IP, service, time и log. Для объяснения этих полей пожалуйста смотрите таблицу 9.3.
4. Нажмите кнопку **Modify** для модификации этого правила ACL. Новые параметры для этого правила ACL отобразятся в таблице контроля доступа внизу страницы настройки ACL.

9.5.3 Удаление правила ACL

Для удаления правила ACL, щелкните иконку напротив правила.

9.5.4 Просмотр правил ACL

Для просмотра существующих правил ACL, откройте страницу настройки правил ACL, щелкнув **Firewall/NAT ->** меню **ACL** и затем выберите направление трафика из выпадающего списка **Traffic Direction**.

9.6 Настройка доступа к роутеру– (Firewall/NAT ->Self-Access ACL)

Правила доступа к маршрутизатору RX3042H. Вы можете использовать страницу настройки правил доступа к роутеру, как показано на рис. 9.7, для:

- Добавления нового правила
- Модификация существующего правила
- Удаление существующего правила
- Просмотра существующих правил

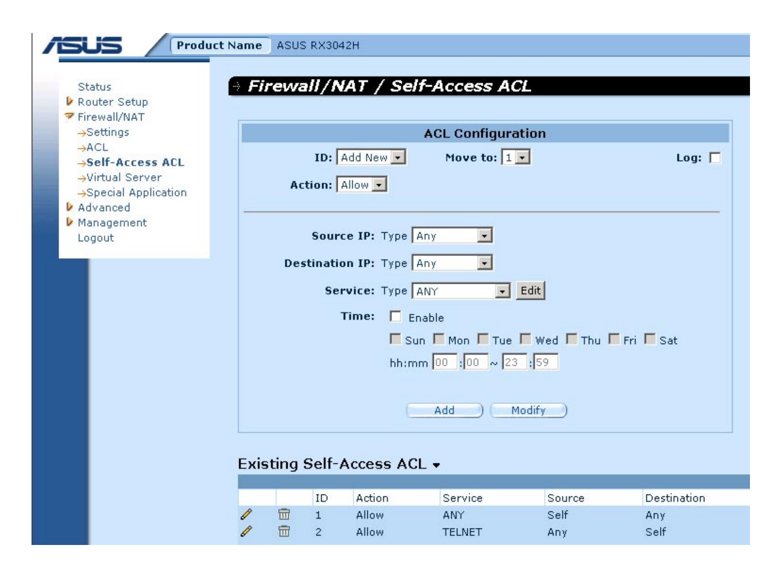


Рис. 9.7. Страница настройки правил доступа к роутеру

9.6.1 Добавление правила доступа к роутеру

Для выполнения правила доступа к роутеру выполните следущее:

1. Откройте страницу настройки правил доступа к роутеру, щелкнув **Firewall/NAT ->** меню **Self-Access ACL**.
2. Выберите “**Add New**” из выпадающего списка “ID”.
3. Выберите желаемое действие (разрешить или отбросить) из выпадающего списка “**Action**”.
4. Присвойте приоритет для этого правила, выбрав номер из выпадающего списка **Move to**. Отметьте, что номер указывает приоритет правила, 1 является наивысшим приоритетом. Правила с высоким приоритетом в брандмауэре проверяются перед правилами с низким приоритетом.
5. Сделайте изменения для любого или всех следущих полей: source/destination IP, service, time и log. Для объяснения этих полей пожалуйста смотрите таблицу 9.3.
6. Нажмите кнопку "**Add**" для создания нового правила доступа к роутеру. Новое правило доступа к роутеру будет отображено в таблице доступа к роутеру внизу страницы настройки правил доступа к роутеру.

Пример

На рис. 9.8 показан образец настройки правила доступа к роутеру, разрешающего любой HTTP-трафик к RX3042H.

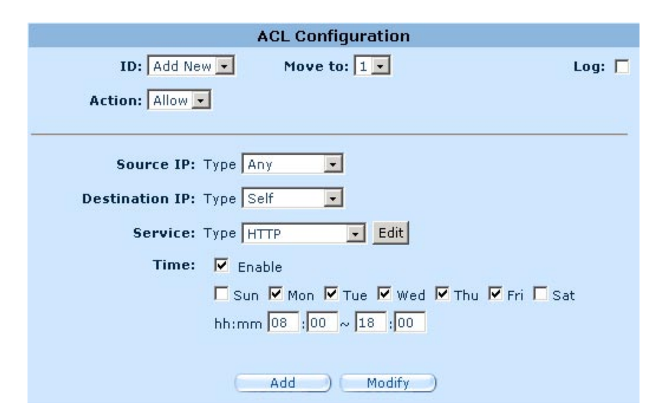


Рис. 9.8. Пример настройки правила доступа к роутеру

9.6.2 Модификация правил доступа к роутеру

Для модификации правила доступа к роутеру выполните следущее:

1. Откройте страницу настройки правил доступа к роутеру, щелкнув **Firewall/NAT ->** меню **Self-Access ACL**.
2. В таблице **Existing Self-Access ACL** нажмите иконку правила доступа к роутеру для его модификации или выберите номер правила из выпадающего списка **ID**.
3. Сделайте изменения для любого или всех следущих полей: source/ destination IP, service, time и log. Для объяснения этих полей пожалуйста смотрите таблицу 9.3.
4. Нажмите кнопку "**Modifiy**" для сохранения изменений. Новые параметры для этого правила доступа появятся в таблице Existing Self-Access ACL, расположенной внизу страницы настройки правил доступа к роутеру.

9.6.3 Удаление правила доступа к роутеру

Для удаления правила доступа к роутеру, щелкните иконку напротив правила.

9.6.4 Просмотр правил доступа к роутеру

Для просмотра правил доступа к роутеру, откройте страницу настройки правил доступа к роутеру, щелкнув **Firewall/NAT ->** меню **Self-Access ACL**.



Existing Self-Access ACL

		ID	Action	Service	Source	Destination
		1	Allow	HTTP	Any	Self
		2	Allow	TELNET	Any	Self

9.7 Настройка виртуального сервера

Виртуальный сервер позволяет вам настроить до десяти публичных серверов, типа Web, E-mail, FTP серверов и других, доступных для внешних пользователей Интернет. Каждая служба обеспечивается выделенным сервером с фиксированным IP адресом. Хотя внутренние адреса серверов непосредственно не доступны для внешних пользователей, маршрутизатор идентифицирует запрос службы по номеру порта и переадресовывает этот запрос на соответствующий внутренний сервер.



Примечание: RX3042H одновременно поддерживает только один сервер любого типа.

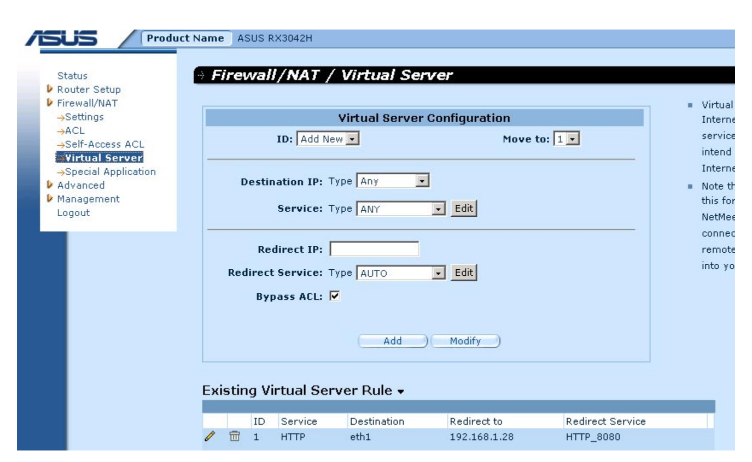


Рис. 9.9. Страница настройки виртуального сервера

9.7.1 Параметры настройки виртуального сервера

В таблице 9.5 описаны параметры настройки для виртуального сервера.

Таблица 9.5. Параметры настройки виртуального сервера

Параметр	Описание
ID	
Add New	Нажмите эту опцию для добавления нового виртуального сервера
Number	Выберите идентификатор виртуального сервера из выпадающего списка для модификации его параметров.
Move to Эта опция позволяет вам установить приоритет для проверки правил виртуального сервера. NAT распределяет IP адреса и/или порты, основываясь на приоритете правил. Установите приоритет, назначив номер для его позиции в списке правил.	
1 (первый)	Этот номер обозначает высший приоритет.
другие числа	Выберите другой номер для указания приоритета, который вы хотите присвоить правилу.
Destination IP Эта опция позволяет вам установить сеть назначения, к которой относится это правило. Выберите одну из следующих опций в выпадающем списке:	
Any	
IP Address	Введите IP адрес виртуального сервера, если виртуальный сервер имеет известный публичный IP адрес.
Interface	Используйте IP адрес выбранного интерфейса как IP адрес назначения. Доступны следущие опции: eth1 (WAN1) eth2 (WAN2) ppp1 (WAN1 – unnumbered) ppp2 (WAN2 – unnumbered) ppp3 (WAN1 – PPPoE 1) ppp4 (WAN1 – PPPoE 2) ppp5 (WAN2 – PPPoE 1) ppp6 (WAN2 – PPPoE 2)
Service	Выберите службу из выпадающего списка, к которой применяется это правило. Если желаемой службы нет в списке, нажмите кнопку Edit для создания новой службы.
Redirect IP	Введите IP адрес компьютера (обычно сервер в вашей сети), к которому вы хотите направить входящий трафик. Например, если IP адрес веб-сервера в вашей сети 192.168.1.28, пожалуйста введите здесь 192.168.1.28.

Параметр	Описание
Redirect Service	Выберите службу из выпадающего списка, к которой применяется это правило. Если требуемой службы нет в списке, нажмите кнопку Edit для создания новой службы.
Bypass ACL	Установите галочку для этой опции, если вы не хотите, чтобы брандмауэр выполнял контроль доступа для этого виртуального сервера. Это означает, что виртуальный сервер разрешает любой доступ к предоставленной службе. Если вы хотите контролировать доступ к этому виртуальному серверу, снимите галочку с этой опции и создайте соответсвующее правило ACL для контроля доступа к виртуальному серверу.

Таблица 9.6. Номера портов для популярных приложений

Приложение	Номера портов
AOE II (Server)	2300-2400
AUTH	113
Baldurs Gate II	2300-2400
Battle Isle	3004-3004
Counter Strike	27005-27015
Cu See Me	7648-7648, 56800, 24032
Diablo II	4000-4000
DNS	UDP 53-53
FTP	TCP 21-21
FTP	TCP 20(ALG)-21
GOPHER	TCP 70-70
HTTP	TCP 80-80
THHP8080	TCP 8080-80880
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500
mirc	66011-700
MSN Messenger	1863 ALG
Need for Speed 5	9400-9400
Netmeeting Audio	TCPP 1731-1731
Netmeeting Call	TCP 1720-1720
Netmeeting Conference	UDP 495000-49700
Netmeeting File Transfer	TCP 1503--1503

Приложение	Номера портов
Netmeeting or VoIP	1503-1503, 1720(ALG)
NEWS	TCP 119-119
PC Anywhere	TCP 5631
PC Anywhere	TCP 5631, UDP 5632
POP3	TCP 110-110
Powwow Chat	13233-13233
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5800

9.7.2 Пример виртуального сервера 1 – Веб-сервер

На рис. 9.10 показана топология сети для для развертывания веб-сервера. Этот веб-сервер предоставляет службу HTTP, используя TCP-порт 8080.

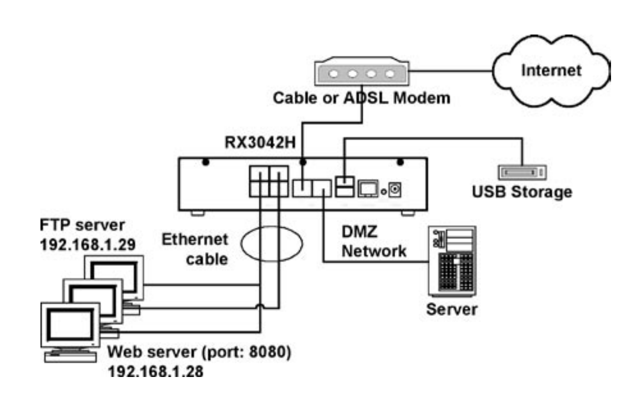


Рис. 9.10. Топология развертывания виртуального сервера

Выполните следущие процедуры для установки веб-сервера, показанного на рис. 9.10.

1. Откройте страницу настройки виртуального сервера, как показано на рис. 9.9, щелкнув **Firewall/NAT** -> меню **Virtual Server**.
2. Выберите тип IP и тип службы как показано на рис. 9.11.

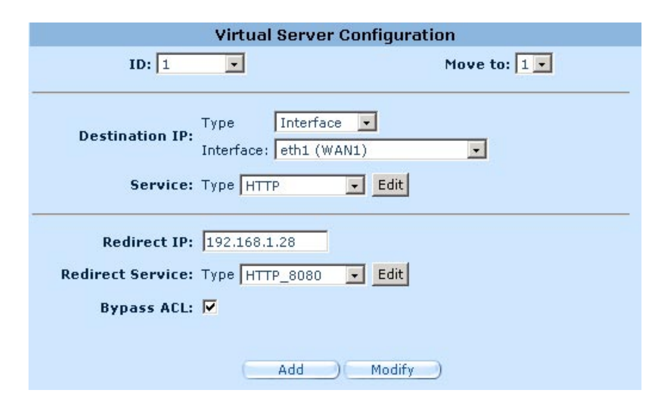


Рис. 9.11. Пример виртуального сервера 1 – Веб-сервер

3. Введите IP адрес веб-сервера, (192.168.1.28), в поле **Redirect IP**.

4. Так как веб-сервер сети не использует стандартный TCP-порт (обычно 80), для http должна быть создана новая служба, использующая 80-ый TCP-порт. Для создания новой службы нажмите кнопку **Edit** на поле переназначения службы. На появившейся странице настройки службы, введите имя службы, протокол и номер порта, как показано на рис. 9.12, затем нажмите **Add to list** для создания новой службы HTTP_8080. Наконец, нажмите кнопку **Save & Exit** для сохранения новой службы.

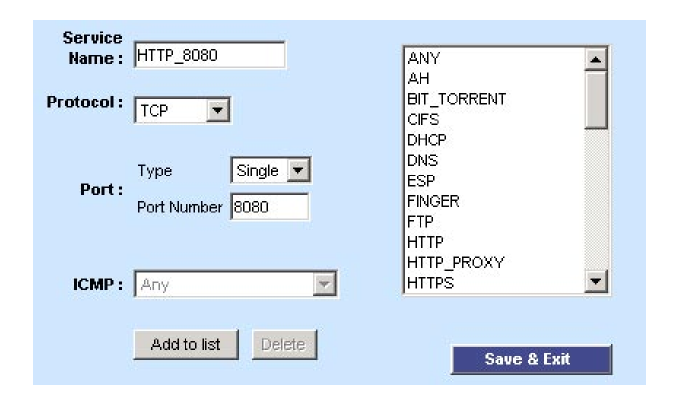


Рис. 9.12. Добавление новой службы

5. Выберите службу, HTTP_8080, из выпадающего списка **Redirect Service**.

6. Нажмите **Add** для сохранения параметров виртуального сервера.

9.7.3 Пример виртуального сервера 2 – FTP сервер

На рис. 9.10 показана топология сети для для развертывания сервера FTP. Этот FTP сервер использует стандартный FTP порт.

Выполните следущие процедуры для установки FTP сервера, показанного на рис. 9.10.

1. Откройте страницу настройки виртуального сервера, как показано на рис. 9.9, щелкнув **Firewall/NAT ->** меню **Virtual Server**.

2. Введите необходимую информацию как показано на рис. 9.13.

3. Нажмите **Add** для сохранения параметров виртуального сервера.

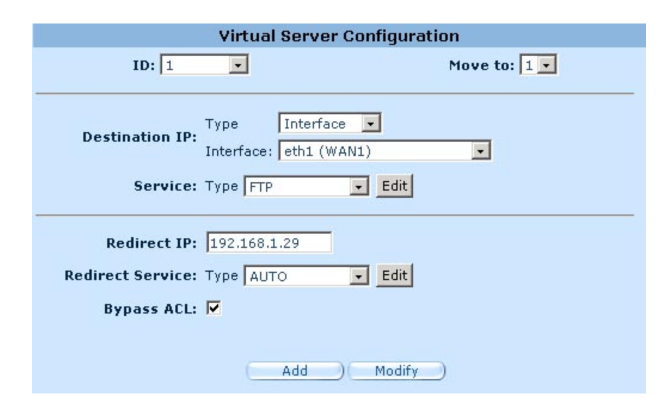


Рис. 9.13. Пример виртуального сервера 3 – FTP сервер

9.7.4 Пример виртуального сервера 3 – FTP сервер с контролем доступа

Этот пример аналогичен предыдущему примеру, описанному в разделе 9.7.3 “Пример виртуального сервера 2 – FTP сервер”, но с контролем доступа, обеспечиваемого ACL-правилами брандмауэра. В этом примере, мы хотим ограничить доступ к FTP серверу для сети 168.192.128.0.

Выполните следущие процедуры для установки FTP сервера.

1. Создайте виртуальный FTP сервер.

a) Откройте страницу настройки виртуального сервера, как показано на рис 9.9, щелкнув **Firewall/NAT ->** меню **Virtual Server**.

b) Введите необходимую информацию, как показано на рис. 9.13.

c) Убедитесь, что галочка **Bypass ACL** снята.

d) Нажмите Add для сохранения параметров виртуального сервера.

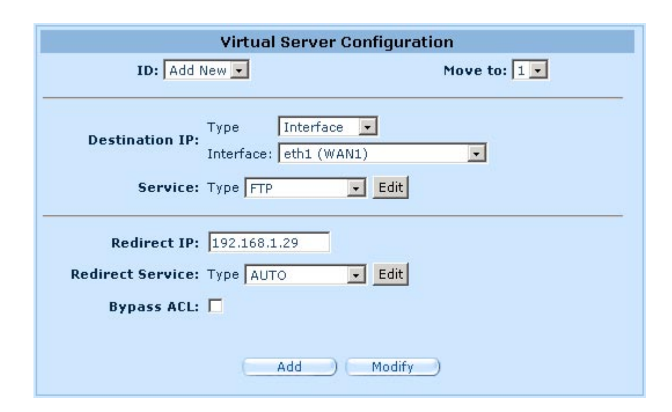


Рис. 9.14. Пример виртуального сервера 3 – FTP сервер

2. Создайте правило ACL для контроля доступа к FTP серверу

a) Откройте страницу настройки правил ACL, как показано на рис. 9.4, щелкнув **Firewall ->** меню **ACL**.

b) Выберите опцию **WAN ->LAN** из выпадающего списка **Traffic Direction**.

c) Выберите **Add New** из выпадающего списка **ID**.

d) Выберите **Allow** из выпадающего списка **Action**.

e) Выберите **Subnet** из выпадающего списка **Source Type**.

f) Введите **168.192.128.0** и **255.255.255.0** для полей **Source Address** и **Mask** соответственно.

g) Выберите **FTP** из выпадающего списка **Service Type**.

h) Присвойте приоритет для этого правила, выбрав номер из выпадающего меню **Move to**. Отметьте, что номер указывает приоритет правила, 1 является высшим. Правила с высоким приоритетом в брандмауэре проверяются до правил с низким приоритетом.

i) Нажмите кнопку **Add** для создания нового правила ACL.

ACL Configuration
Traffic Direction: WAN -> LAN
ID: Add New
Move to: 1
Log:
Action: Allow
Source: Type Subnet
Address 168.192.128.0
Mask 255.255.255.0
Destination: Type Any
Service: Type FTP
Edit
Time: Enable
Sun Mon Tue Wed Thu Fri Sat
hh:mm 00 : 00 ~ 23 : 59
Add
Modify

Рис. 9.15. Пример правил брандмауэра для виртуального сервера 3 – FTP сервер

9.8 Настройка специальных приложений

Некоторые приложения используют несколько TCP/UDP портов для передачи данных. Из-за NAT, эти приложения не могут работать с роутером. Настройка специальных приложений позволяет этим приложениям корректно работать.



Примечание: Одновременно только один ПК может использовать специальные приложения...

9.8.1 Параметры настройки специальных приложений

В таблице 9.7 приведены параметры, доступные для настройки виртуального сервера.

Таблица 9.7. Параметры насройки специальных приложений

Параметр	Описание
Enabled	Установите галочку для включения приложения.
Trigger Protocol	Выберите протокол из выпадающего списка. Доступны TCP, UDP и TCP/UDP.
Outgoing (Trigger) Port	Диапазон портов для отправки исходящих пакетов. Номера исходящих портов действуют как триггер. Когда роутер обнаружит исходящие пакеты с номерами этих портов, он разрешит соответствущим входящим пакетам с номерами входящих портов, определенных в поле Incoming Port, пройти через роутер. Список портов наиболее популярных приложений приведен в таблице 9.8
Incoming Protocol	Протокол, используемый входящими пакетами. Доступны TCP, UDP и TCP/UDP.
Incoming Port	Диапазон портов для входящих пакетов. Список портов наиболее популярных приложений приведен в таблице 9.8. Отметьте, что диапазон портов указывается парой цифр, разделенных тире, например: 100-200. Несколько диапазонов разделяются запятой, например: 100-200, 700-800.
Comment	Здесь вы можете ввести описание для приложения, например имя, идентифицирующее приложение.

Таблица 9.8. Номера портов для популярных приложений

Приложение	Диапазон исходящих портов	Диапазон входящих портов
Battle.net	6112	6112
DialPad	7175	51200, 51201, 51210
ICU II	2019	2000-2038, 2050-2051, 2069, 2085, 3010-3030
MSN Gaming Zone	47624	2300-2400, 28800-29000
PC to Phone	12053	12120, 12122, 150-24220
Quick Time 4	554	6970-6999
wowcall	8000	4000-4020
Yahoo Messenger	5050	5000-5101

9.8.2 Пример специального приложения

Рис. 9.16. Страница настройки специальных приложений

Ниже приведена процедура установки специального приложения для MSN Gaming Zone.

1. Откройте страницу настройки специальных приложений, как показано на рис. 9.16, щелкнув **Firewall/NAT ->** меню **Special Application**.
2. Установите галочку **Enabled**.
3. Выберите **TCP/UDP** из выпадающего списка **Trigger Protocol**. Если вы не уверены какой из протоколов использует приложение, вы можете выбрать TCP/UDP.
4. Введите диапазон исходящих портов, в этом случае: 47624 ~ 47624.
5. Выберите **TCP/UDP** из выпадающего списка **Incoming Protocol**. Если вы не уверены какой из протоколов использует приложение, вы можете выбрать TCP/UDP.
6. Введите диапазон входящих портов, в этом случае: 2300-2400 и 28800-29000
7. В поле **Comment** введите аписание для этого приложения, для этого примера MSN Gaming Zone.
8. Нажмит**е Appl**y для сохранения параметров.

10 Управление системой

В этой части описаны административные задачи, которые вы можете выполнить, используя менеджер конфигурации:

- Настройка системных служб
- Изменение пароля и настройка параметров системы
- Просмотр системной информации
- Изменение системной даты и времени
- Настройка SNMP
- Сброс к заводским установкам
- Сохранение и восстановление конфигурации системы
- Перезагрузка
- Обновление прошивки

10.1 Настройка системных служб

Вы можете использовать страницу настройки системных служб для включения или выключения служб, поддерживаемых RX3042H, как показано на рис. 10.1. Все службы, кроме DDNS, SNTP, UPnP и RIP, включены на заводе. Для включения или выключения службы выполните следующее:

1. Откройте страницу настройки системных служб, щелкнув **Management ->** меню **System Services**.
2. Выберите **Enable** или **Disable** для включения или отключения желаемой службы.
3. Нажмите кнопку **Apply** для сохранения изменений.

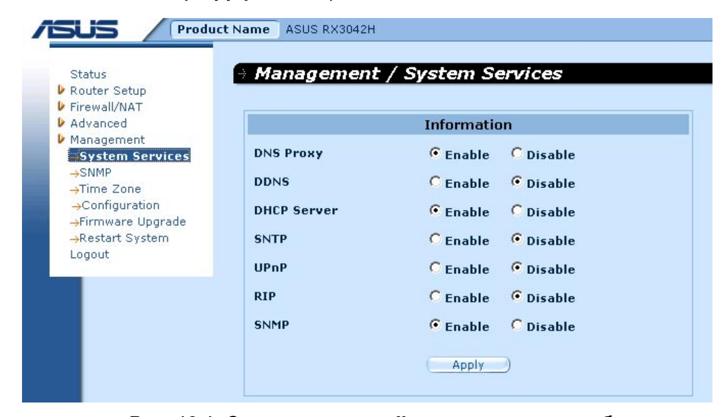


Рис. 10.1. Страница настройки системных служб

10.2 Пароль и параметры системы

10.2.1 Изменение пароля

Имя и пароль по умолчанию для входа в менеджер конфигурации (admin и admin). В целях безопасности, желательно чтобы вы сменили пароль во избежание несанкционированных изменений в настройках роутера.



Примечание: Это имя пользователя и пароль используются только для входа в менеджер конфигурации; это не тот пароль, который вы используете для подключения к вашему провайдеру.

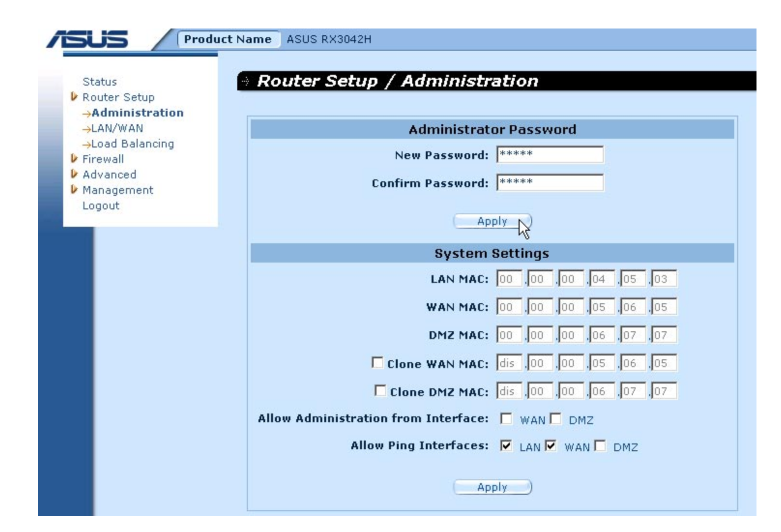


Рис. 10.2. Страница администрирования

Для изменения пароля выполните следующее:

1. Откройте страницу администрирования, как проказано на рис. 10.2, щелкнув **Router Setup ->** меню **Administration**.

2. Измените пароль

a) Введите новый пароль в поле **New Password** и еще раз в поле **Confirm Password**. Пароль может быть до 16 символов. При входе в менеджер конфигурации, вы должны ввести новый пароль в том же регистре в каком ввели здесь.

3. Нажмите кнопку **Apply** для сохранения нового пароля.

10.2.2 Настройка параметров системы

Для изменения параметров системы выполните следующее:

1. Откройте страницу администрирования, как показано на рис. 10.2, щелкнув **Router Setup ->** меню **Administration**.

2. Клонирование MAC адреса для WAN
   Если вы прежде зарегистрировали определенный MAC у вашего провайдера для доступа к Интернет, установите галочку **Clone WAN MAC** и введите зарегистрированный MAC адрес.

3. Allow Administration from WAN: установите или снимите галочку для включения или отключения удаленного управления через порт WAN.

4. Allow Ping Interface: Эта опция позволяет пользователю проверять доступ к роутеру, используя **ping** через порты LAN или WAN. Установите соответствующую галочку для разрешения ping на соответствующем интерфейсе.

5. Нажмите кнопку **Apply** для сохранения параметров.

10.3 Просмотр системной информации

Страница состояния системы отображается при каждом входе в менеджер конфигурации. Также для просмотра страницы состояния вы можете щелкнуть меню **Status.** На этой странице показаны общие параметры системы.

ASUS Product Name ASUS RX3042H

Status

Status
Router Setup
Firewall
Advanced
Management
Logout

General Information

System Name: RX3042H
Firmware Version: 0.53
System Time: 18:35:23 5 5 2005
Default Gateway: 172.21.150.1

LAN Information

IP Address: 192.168.1.1
Netmask: 255.255.255.0
MAC Address: 00-00-00-04-05-03

WAN Information

Connection Mode: DHCP
IP Address: 172.21.151.13
Netmask: 255.255.254.0
Gateway: 172.21.150.1
DNS Server1: 172.21.128.8
DNS Server2: 172.21.128.9
MAC Address: 00-01-02-03-10-FF

DMZ Information

Connection Mode: Static
IP Address: 192.168.3.1
Netmask: 255.255.255.0
Gateway: 192.168.3.254
DNS Server1: 192.168.3.254
DNS Server2: 0.0.0.0
MAC Address: 00-00-00-06-07-07

Рис. 10.3. Страница состояния системы

10.4 Установка даты и времени

RX3042H ведет учет текущей даты и времени, которые используются для вычисления и сообщения различных данных. Хотя в RX3042H имеются часы реального времени; вы, для получения правильного времени, также можете использовать внешние сервера точного времени. RX3042H позволяет вам настроить до трех внешних серверов точного времени. Для включения протокола SNTP (протокол синхронизации времени) установите галочку **SNTP Enable**.



Примечание: Изменение даты и времени в RX3042H не влияет на дату и время в ваших ПК.

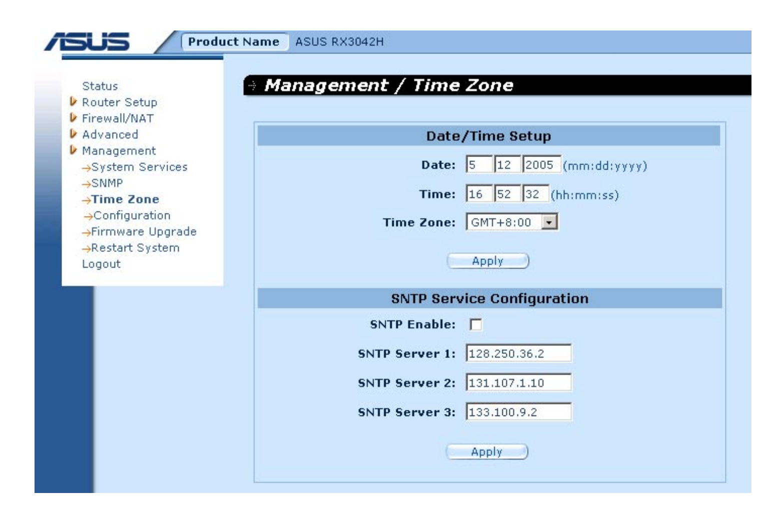


Рис. 10.4. Страница настройки времени

Для ручного изменения времени в роутере:

1. Откройте страницу настройки времени, щелкнув **Management ->** меню **Time Zone**.
2. Введите текущую дату и время в соответствующие поля.
3. Выберите ваш часовой пояс из выпадающего списка.
4. Нажмите кнопку **Apply** для сохранения параметров.

Для синхронизации времени между часами реального времени и внешними серверами точного времени:

1. Откройте страницу настройки времени, щелкнув **Management ->** меню **Time Zone**.
2. Выберите ваш часовой пояс из выпадающего списка.
3. Установите галочку **SNTP Enable** для включения службы SNTP.
4. Введите IP адреса для серверов SNTP, которые будут использоваться для обновления системного времени.
5. Нажмите кнопку **Apply** для сохранения параметров.

10.4.1 Просмотр системной даты и времени

Для просмотра даты и времени, войдите в менеджер конфигурации,

щелкнув **Management ->** меню **Time Zone**.

10.5 Настройка SNMP

SNMP (простой протокол управления сетью) используется для управления сетью. Вы можете использовать страницу настройки SNMP для включения или отключения протокола SNMP.

10.5.1 Параметры настройки SNMP

В таблице 10.1 приведены параметры настройки для SNMP.

Таблица 10.1. Параметры настройки SNMP

Поле	Описание
SNMP Enable	Установите галочку для включения SNMP; в противном случае снимите ее.
RO Community Name	Строка сообщества - это текстовая строка, которая используется как пароль между станцией управления SNMP и роутером. Это "только для чтения" общественное имя используется станцией управления SNMP для чтения параметров роутера.
RW Community Name	Строка сообщества - это текстовая строка, которая используется как пароль между станцией управления SNMP и роутером. Это "чтение и запись" общественное имя используется станцией управления SNMP для чтения и настройки параметров роутера.
Trap Address	Trap-сообщение, посылаемое роутером для сообщения станции управления SNMP, что в роутере что-то случилось. Это поле используется для ввода IP адреса станции управления SNMP, которая поддерживает прием trap-сообщений от роутера.

10.5.2 Настройка SNMP

1. Откройте страницу настройки SNMP, как показано на рис. 10.5, щелкнув **Management ->** меню **SNMP**.

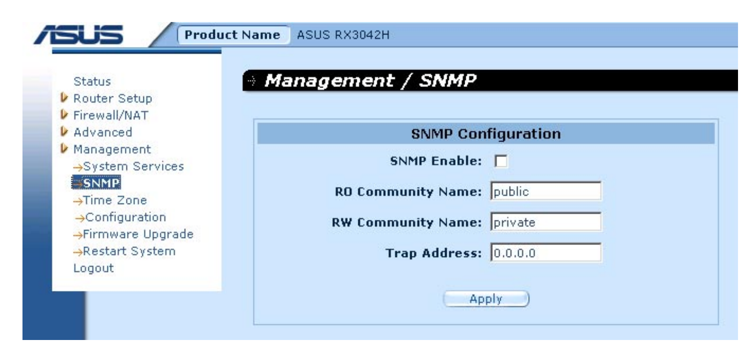


Рис. 10.5. Страница настройки SNMP

2. Установите или снимите галочку **SNMP Enable** для включения или отключения SNMP.
3. Введите общественные имена **RO** (только для чтения) и **R/W** (чтение и запись).
4. Введите IP адрес станции управления SNMP, которая принимает trap-сообщения от роутера.
5. Нажмите кнопку **Apply** для сохранения параметров.

10.6 Настройка журнала

Сообщения журнала хранятся в динамической памяти и исчезают после перезагрузки системы. Для сохранения сообщений, вы можете установить syslog сервер и RX3042H будет посылать сообщения на сервер.

10.6.1 Настройка удаленного журнала, используя syslog сервер

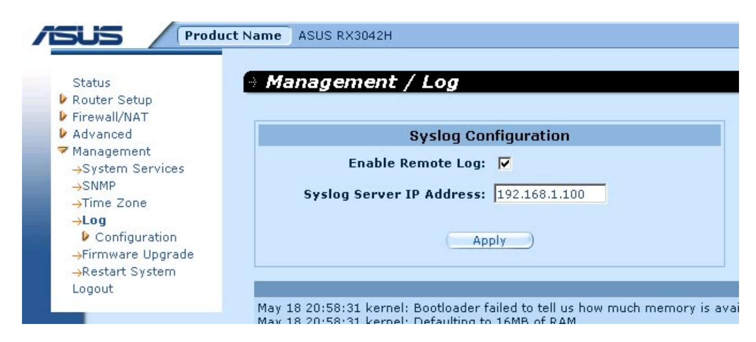


Рис. 10.6. Настройка syslog сервера

1. Откройте страницу настройки журнала, как показано на рис. 10.6, щелкнув **Management ->** меню **Log**.
2. Установите галочку **Enable Remote Log** для включения удаленного журнала.
3. Введите IP адрес syslog сервера в поле **Syslog Server IP Address**.
4. Нажмите кнопку **Apply** для сохранения параметров.

10.6.2 Просмотр системного журнала

Вы можете открыть журнал для просмотра, щелкнув **Firewall/NAT ->** меню **Log**. На рис. 10.7 показан образец журнала. Для просмотра обновленных сообщений вы можете нажать кнопку **Reload** внизу страницы. Для очистки журнала от сообщений нажмите кнопку **Clear Log**.

```
May 19 19:47:21 kernel: fw: SELF rule=1 allow udp from 172.21.150.29 to 172.21.151.255 sport=138 dport=138
May 19 19:47:25 kernel: fw: SELF rule=1 allow icmp from 192.168.1.1 to 192.168.1.11 type=8 code=0 id=155
May 19 19:47:29 kernel: fw: SELF rule=1 allow udp from 172.21.151.15 to 172.21.151.255 sport=5003 dport=5003
May 19 19:47:31 kernel: fw: SELF rule=1 allow udp from 172.21.150.12 to 172.21.151.255 sport=138 dport=138
May 19 19:47:31 kernel: fw: SELF rule=1 allow udp from 172.21.151.15 to 172.21.151.255 sport=138 dport=138
May 19 19:47:32 kernel: fw: SELF rule=1 allow udp from 172.21.150.35 to 172.21.151.255 sport=138 dport=138
May 19 19:47:40 kernel: fw: SELF rule=1 allow udp from 172.21.150.22 to 172.21.151.255 sport=138 dport=138
May 19 19:47:43 kernel: fw: SELF rule=1 allow udp from 172.21.150.26 to 172.21.151.255 sport=138 dport=138
May 19 19:47:43 kernel: fw: SELF rule=1 allow udp from 172.21.150.8 to 172.21.151.255 sport=138 dport=138
May 19 19:47:44 kernel: fw: SELF rule=1 allow udp from 172.21.150.10 to 172.21.151.255 sport=138 dport=138
May 19 19:47:44 kernel: fw: SELF rule=1 allow udp from 172.21.150.34 to 172.21.151.255 sport=138 dport=138
May 19 19:47:54 kernel: fw: SELF rule=1 allow udp from 172.21.151.9 to 172.21.151.255 sport=138 dport=138
May 19 19:47:54 kernel: fw: SELF rule=1 allow udp from 172.21.151.36 to 172.21.151.255 sport=138 dport=138
May 19 19:47:56 kernel: fw: SELF rule=1 allow udp from 172.21.150.28 to 172.21.151.255 sport=138 dport=138
```

Reload | Clear Log

Рис. 10.7 Образец журнала

10.7 Управление конфигурацией

10.7.1 Восстановление заводских параметров устройства

Иногда, вы возможно захотите восстановить заводские параметры для устранения проблем, произошедших из-за неправильной конфигурации системы. Для восстановления заводских параметров выполните следующее:

1. Откройте страницу сброса к заводским параметрам по умолчанию, как показано на рис. 10.8, щелкнув **Management ->Configuration ->** меню **Factory Default**.

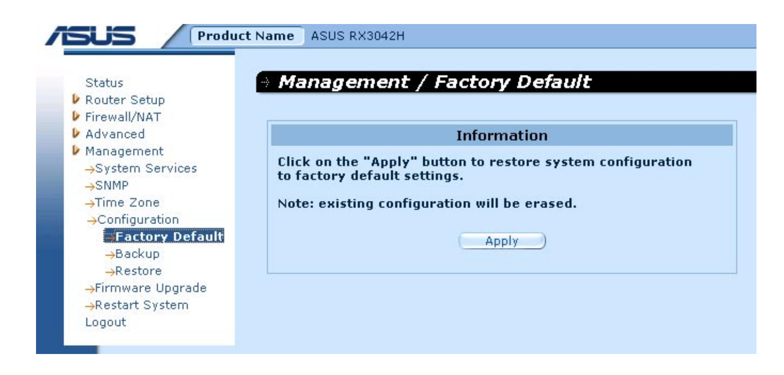


Рис. 10.8 Страница сброса к заводским параметрам

2. Нажмите кнопку **Apply** для восстановления заводских параметров устройства.

3. Появится диалоговое окно, как показано на рис. 10.9. Нажмите кнопку **OK** для продолжения; или нажмите кнопку **Cancel** для отмены действия.

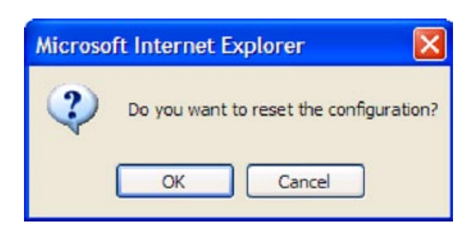


Рис. 10.9 Подтверждение сброса к заводским парамерам

4. RX3042H должен перезагрузится, чтобы значения по умолчанию дали эффект. Таймер обратного отсчета, как показано на рис. 10.10, показывает сколько времени осталось до завершения процесса перезагрузки.



Рис. 10.10 Таймер обратного отсчета при сбросе к заводским параметрам

Иногда, вы можете обнаружить, что не имеете доступа к RX3042H, например, вы забыли ваш пароль или IP адрес RX3042H. Единственный выход из этой ситуации -это сброс системы к заводским параметрам. Для этого нажмите и удерживайте кнопку reset более 5 секунд. После перезагрузки RX3042H будут установлены заводские параметры по умолчанию.

10.7.2 Резервное копирование конфигурации системы

Для резервного копирования конфигурации системы выполните следующее:

1. Откройте страницу резервного копирования конфигурации системы, щелкнув **Management ->Configuration ->** меню **Backup**.
2. Нажмите кнопку **Apply** для резервного копирования конфигурации.

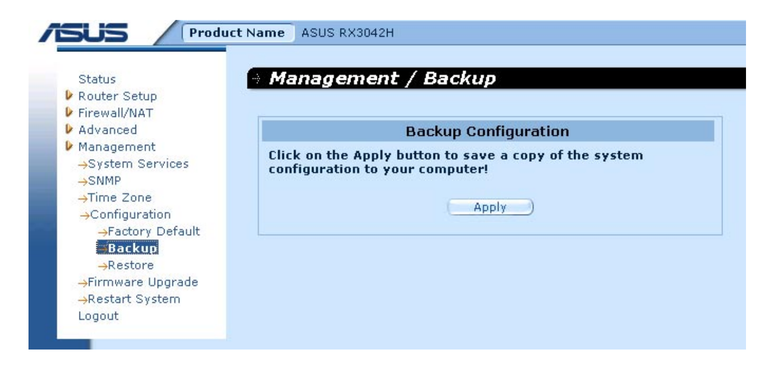
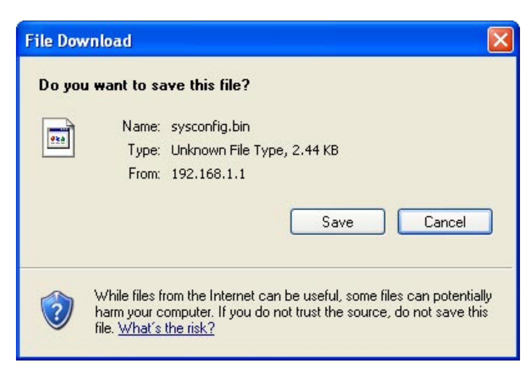
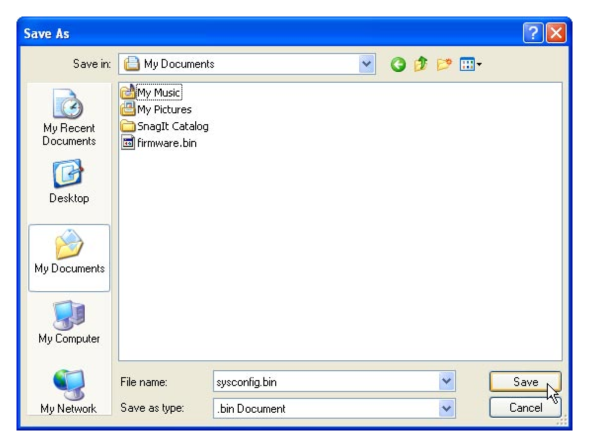


Рис. 10.11 Страница резервного копирования конфигурации

3. Нажмите кнопку **Save** для подтверждениярезервного копирования конфигурации.



4. Нажмите кнопку **Save** для сохранения конфигурации



10.7.3 Восстановление конфигурации системы

Для восстановления конфигурации системы выполните следущее:

1. Откройте страницу восстановления конфигурации системы,как показано на рис. 10.12, щелкнув **Management ->Configuration ->** меню **Restore**.

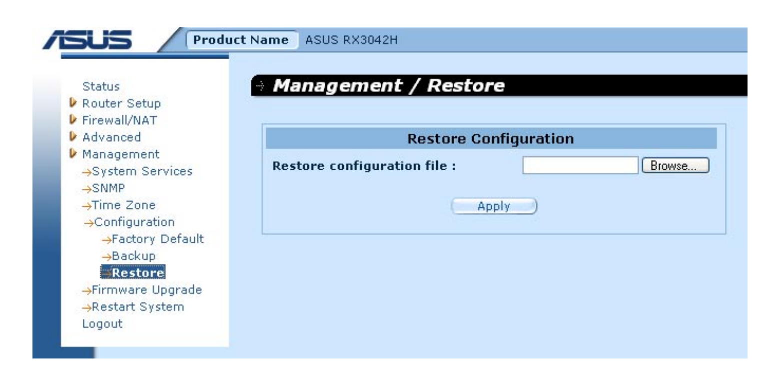


Рис. 10.12 Страница восстановления конфигурации системы

2. Введите путь и имя файла конфигурации ситемы в поле **Configuration File**. Также вы можете нажать кнопку **Browse...** для поиска файла конфигурации системы на вашем жестском диске. Для выбора файла конфигурации системы появится окно, аналогичное показанному на рис. 10.13. Выберите файл и нажмите кнопку **Open.**

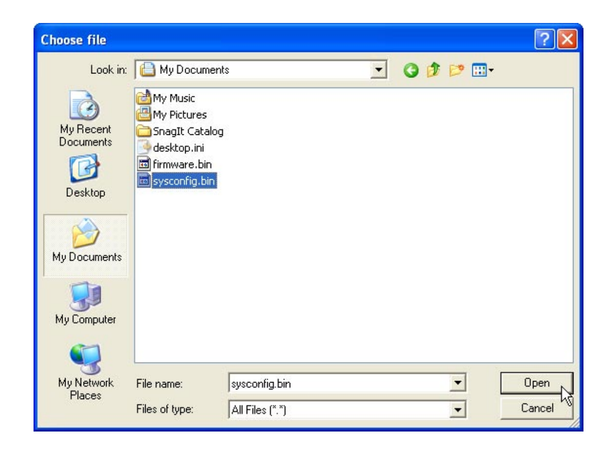


Рис. 10.13 Выбор файла конфигурации системы

3. Нажмите кнопку **Apply** для восстановления конфигурации системы. Появится диалоговое окно, как показано на рис. 10.14, запрашивающее подтверждения для восстановления системы. Нажмите кнопку **OK** для продолжения; или нажмите кнопку **Cance**l для отмены действия. Отметьте, что для использования новой конфигурации RX3042H должен перезагрузиться.

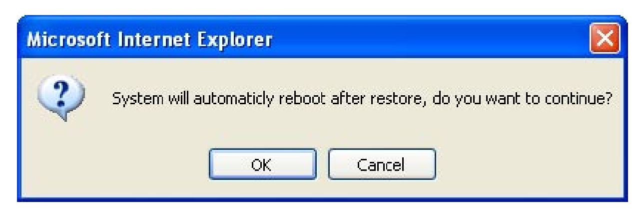


Рис. 10.14 Подтверждение восстановления конфигурации

4. При перезагрузке появится таймер обратного отсчета, как показано на рис. 10.15. Вы будете подключены обратно к RX3042H когда таймер дойдет до нуля. Если вы автоматически не подключитесь обратно к RX3042H, возможно вам придется вручную подключиться обратно к RX3042H.

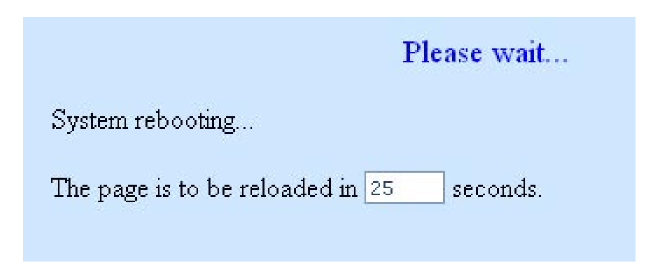


Рис. 10.15 Таймер обратного отсчета при восстановлении системы

10.8 Обновление прошивки

ASUSTeK может время от времени обновлять прошивку для RX3042H. Все программное обеспечения находится в единственном файле, который называется образ. Менеджер конфигурации предоставляет легкий путь для обновления прошивки. Для обновления выполните следущее:

1. Откройте страницу обновление прошивки, как показано на рис. 10.16, щелкнув **System ->** меню **Firmware Upgrade**.

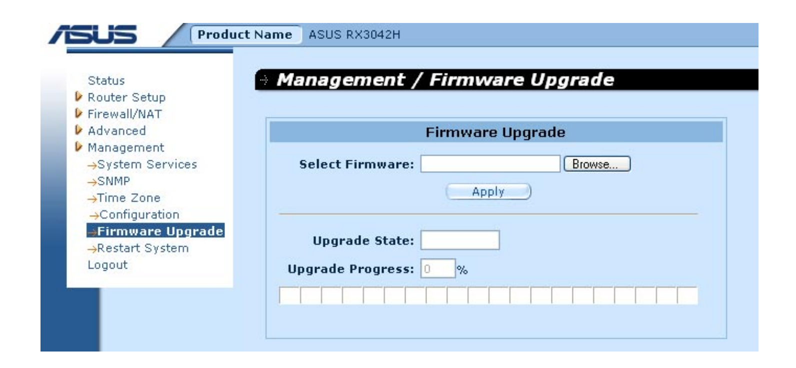


Рис. 10.16 Страница обновления прошивки

2. В поле **Select Firmware** введите путь и имя файла-образа. Также вы можете нажать кнопку **Browse...** для открытия менеджера файлов, показанного на рис. 10.17, для поиска образа на вашем компьютере.

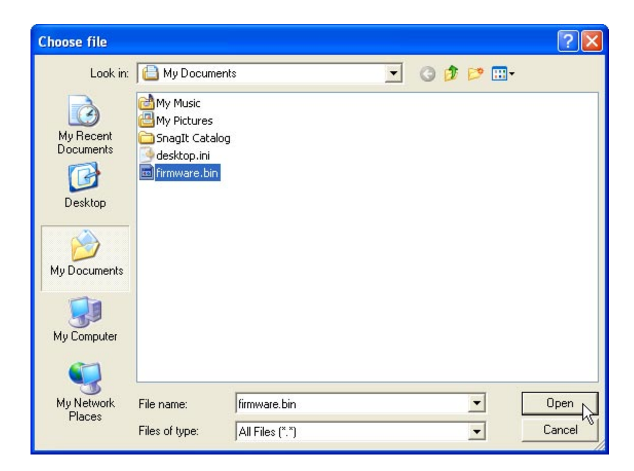


Рис. 10.17 Выбор прошивки в менеджере файлов

3. Нажмите кнопку **Apply** для обновления прошивки. Появится диалоговое окно, как показано на рис. 10.18, запрашивающее подтверждение для обновления прошивки. Нажмите кнопку **OK** для продолжения; или нажмите кнопку **Cance**l для отмены действия.

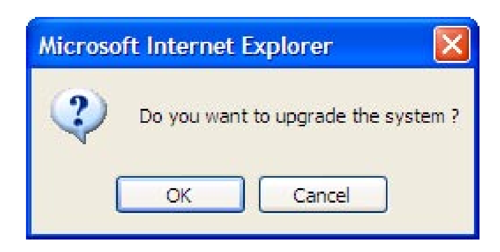


Рис. 10.18 Подтверждение обновления прошивки

4. Появится окно, показывающее состояние и прогресс обновления прошивки, как показано на рис. 10.19

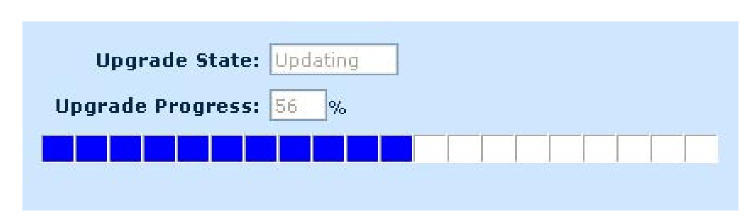


Рис. 10.19 Прогресс обновления прошивки

5. После завершения обновления появится таймер обратного отсчета, как показано на рис. 10.20. Вы будете подключены обратно к RX3042H когда таймер дойдет до нуля. Если вы автоматически не подключитесь обратно к RX3042H, возможно вам придется вручную подключиться обратно к RX3042H.

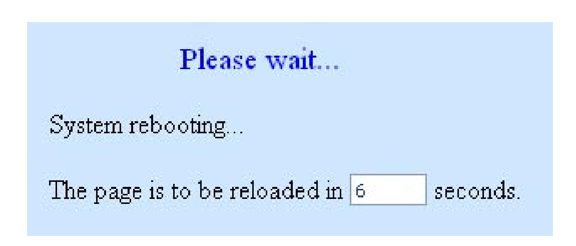


Рис. 10.20 Таймер обратного отсчета при обновлении прошивки

6. Когда вы подключились к RX3042H, нажмите меню **Status** и проверьте, что обновление прошивки прошло правильно. Отметьте, что для просмотра обновленной страницы состояния системы вам, возможно, нужно очистить кеш вашего браузера. Для очистки кеша браузера Microsoft Internet Explorer выполните следущее:

a) Нажмите меню **Tools**

b) Нажмите меню **Internet Options...**

c) Нажмите кнопку **Delete Files...** для очистки кеша браузера.

10.9 Перезагрузка системы

1. Откройте страницу перезагрузки системы, как показано на рис. 10.21, щелкнув **Management ->** меню **Restart System**.

2. Нажмите кнопку **Apply** для перезагрузки системы.

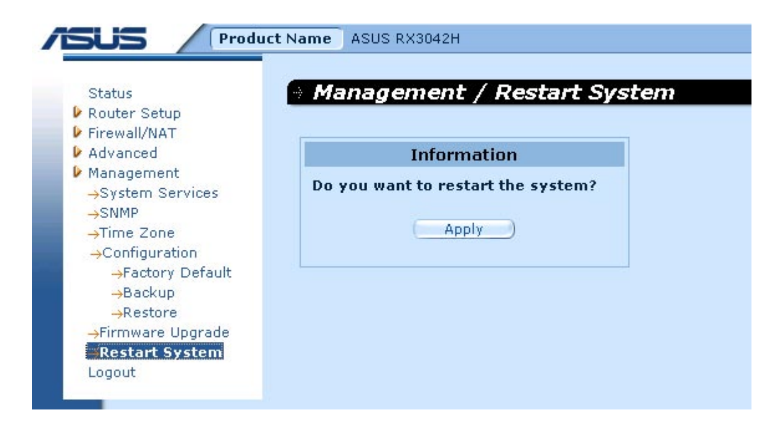


Рис. 10.21 Страница перезагрузки системы

10.10 Выход из менеджера конфигурации

Для выхода из менеджера конфигурации, откройте страницу выхода из системы, как показано на рис. 10.22, щелкнув меню **Logout** и нажав кнопку **Apply**. Если вы используете браузер IE, появится окно как на рис. 10.23.

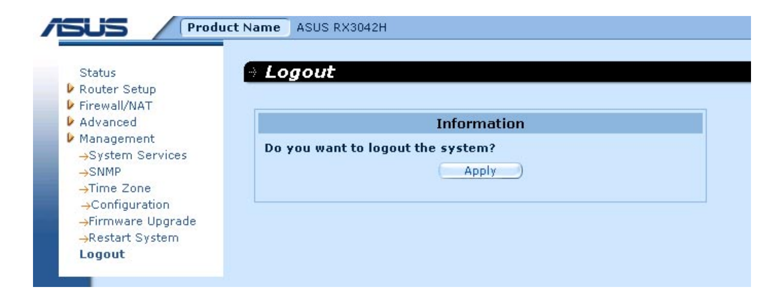


Рис. 10.22 Страница выхода из менеджера конфигурации



Рис. 10.23 Подтверждение закрытия браузера (IE)

11 USB приложение

В этой главе описано как настроить сетевой устройство хранения данных USB для совместного использования ваших данных через службу FTP. В RX3042H интегрирован сервер FTP для устройства хранения данных USB. Перед использованием сервера FTP, убедитесь, что ваше устройство USB соответствует следующим требованиям.

- Поддерживаются только HDD и флеш-диски. Приводы CD-ROM и DVD не поддерживаются. Список совместимых устройств пожалуйста смотрите на http://support.asus.com/.
- Поддерживаются функции чтение/запись для файловых систем FAT/FAT32 и Linux EXT2. Файловая система NTFS не поддерживается.
- Устройства со множеством разделов могут быть определены; но только первые пять разделов будут доступны.



RX3042H поддерживает только устройства USB распознанные как “Mass Storage Device”, такие как HDD и флеш-диски. Большинство устройств USB являются "plug and play"; при подключении этих устройств вам не нужно отключать питание маршрутизатора.

11.1 Настройка устройств USB

Для настройки сетевого устройства выполните следущие инструкции:

1. Убедитесь, что ваше устроство USB включено и подключено к одному из USB портов на задней стороне роутера.
2. Откройте страницу сетевое хранилище, щелкнув **USB Application ->** меню **Network Storage**.
3. Для доступа к устройству USB выберите соответствующий язык из выпадающего меню **Character Set**. Если ваше устройство USB содержит только английские символы, пожалуйста выберите English.
4. Если необходимо установите службу FTP. Отметьте, что если служба FTP не запущена, устройство USB будет недоступно. Для конфигурации FTP сервера, щелкните кнопку **Configure** и следуйте инструкциям, описанным в разделе 11.3 “Настройка службы FTP”.



Рис. 11.1 Сетевое хранилище - опции

Таблица 11.1 Настройка сетевого хранилища

Поле	Описание
Mount options - character set	Для доступа к устройству USB выберите соответствующий язык. Если ваше устройство USB содержит упрощенные китайские символы, выберите упрощенный китайский язык. Доступные опции упрощенный китайский, традиционный китайский и английский.
Device	Поддерживаются два устройства USB.
Information	В этом поле показана информация о поставшике устройства USB. Для подробной информации об устройстве щелкните на иконке .
Status	Disconnected: нет подключенного устройства Connected: устройство подключено, но не используется. Вы можете увидеть это состояние когда устройство не настроено или файловая система устройсва не поддерживается. Mounted: устройство подключено и используется Отметьте, что система не устанавливает подключенные устройства USB автоматически, даже при запущенном FTP сервере и поддерживаемой файловой системе устройства.
Action	Mount: делает устройство USB доступным для маршрутизатора, в противном случае FTP сервер не может обратиться к нему. Unmount: разгрузить устройство USB так, что устройство можно безопасно отключить.

11.2 Просмотр состояния подключенного устройства USB

Для просмотра состояни подключенного устройства USB, следуйте следущим инструкциям:

1. Откройте страницу сетевое хранилище, щелкнув **USB Application ->** меню **Network Storage**.
2. Нажмите кнопку **Reload** для просмотра обновленного состояния подключенных устройств USB. Для подробной информации нажмите кнопку .

11.3 Настройка службы FTP

Для настройки службы FTP выполните следущие инструкции:

1. Откройте страницу сетевое хранилище, щелкнув **USB Application ->** меню **Network Storage**.
2. Нажмите кнопку **Configure** для настройки службы FTP.
3. Установите желаемые опции. Подробности описаны в таблице 11.2 Настройка FTP сервера.
4. (опционально) Введите имя пользователя и пароль, а таже выберите желаемые права доступа из выпадающего списка. Эта опция необходима в том случае, когда доступ к устройству USB разрешается только определенным пользователям.
5. Для сохранения параметров назмите кнопку **Apply**.



Рис. 11.2 Сетевое хранилище - параметры FTP сервера

Table 11.2. Настройка FTP сервера

Параметр	Описание
Status	ON: FTP сервер активен OFF: FTP сервер выключен
Enable FTP server	Установите галочку для включения FTP сервера. Отметьте, что система установивит подключенные устройства USB автоматически, если запущен FTP сервер.
Allow Anonymous User to Login	Выберите это, если вы разрешаете доступ к FTP серверу анонимным пользователям с правами только чтение. Имя пользователя anonymous или ftp. Пароль не требуется.
Allow User from Anywhere	Выберите это, если вас не волнует местоположение клиентов. Если вы не выбрали эту опцию, вам нужно настроить Firewall/ NAT-> Sef-Access ACL для контроля доступа к FTP серверу. Например: разрешить вашей сети 192.168.1.0/24 доступ к FTP серверу.
Maximum Users Allowed to Login	Введите максимальное количество пользователей, использующих FTP сервер одновременно. Максимальное количество пользователей - 10.
Accessible Drives	Выберите одну из опций доступа к диску для FTP сервера. Параметры по умолчанию USB1+USB2. Выберите First Partition если вы хотите обращаться только к первому разделу. Выберите USB1+USB2 если вы хотите обращаться ко всем разделам USB1 и USB2. Выберите USB1 если вы хотите обращаться ко всем разделам USB1. Выберите USB2 если вы хотите обращаться ко всем разделам USB2.

Таблица 11.3. Установка учетной записи пользователя

Параметр	Описание
User name	Введите имя пользователя для доступа к FTP
Password	Введите пароль для доступа к FTP
Rights	Это поле показывает права доступа этого FTP : Read/Write/Delete: Пользователи с этим уровнем доступа могут читать, писать и удалять файлы. Read/Write: Пользователи с этим уровнем доступа могут читать, писать но не могут удалять файлы. Read Only: Пользователи с этим уровнем доступа могут только читать файлы.

11 IP адреса, сетевые маски и подсети

11.1 IP адреса



Примечание: Этот раздел относится только к IP адресам для IPv4 (4-я версия интернет-протокола). Не относится к адресам IPv6.

В этом разделе предоставлены основные понятия о двоичной ситеме счисления, битам и байтам.

IP адресация, интернет-версия телефонных номеров, используется для определения индивидуальных узлов (компьютеров или устройств) в интернет. Каждый IP адрес содержит четыре числа, каждое в диапазоне от 0 до 255, разделенных точками, например: 20.56.0.211. Эти числа называют слева направо, поле1, поле2, поле3, поле4.

Этот стиль записи IP адресов как десятичных цифр, разделееных точками называют десятично-точечной записью. IP адрес 20.56.0.211 читается "двадцать точка пятьдесятшесть точка ноль точка два одиннадцать."

11.1.1 Структура IP адреса

IP адреса имеют иерархию подобно телефонным номерам. Например, 7-ми значный телефонный номер начинается с 3-х значного префикса, который определяет группу из тысячи телефонных линий, и в конце четыре цифры определяют линию в этой группе.

Аналогично, IP адреса имеют два типа информации.

- ID сети

  Определяет сеть в интернет или интранет

- ID узла

  Определяет конкретный компьютер или устройство в сети

Первая часть каждого IP адреса содержит ID сети, остальная часть адреса содержит ID узла. Длина ID сети зависит от класса сети (см. следующий раздел). В таблице 11.1 показана структура IP адреса.

Таблица 11.1. Структура IP адреса

	Поле 1	Поле 2	Поле 3	Поле 4
Класс A	ID сети	ID узла		
Класс B	ID сети		ID узла	
Класс C	ID сети			ID узла

Примеры правильных IP адресов:

Класс A: 10.30.6.125 (сеть = 10, узел = 30.6.125)

Класс B: 129.88.16.49 (сеть = 129.88, узел = 16.49)

Класс C: 192.60.201.11 (сеть = 192.60.201, узел = 11)

11.2 Классы сетей

Три наиболее часто используемых класса сетей A, B и C. (Имеется также класс D, но он предназначен для специального использования и выходит за рамки данного обсуждения.) Эти классы имеют различное предназначение и характеристики.

Сети класса A являются огромными интернет-сетями, каждая имеет свыше 16 миллионов узлов. Этих больших сетей может быть до 126, с общим количеством узлов более 2 миллиардов. Из-за больщих размеров эти сети используются для глобальных сетей и организаций с интернет-инфраструктурой, например интернет-провайдерами.

Сети класса B меньше каждая имеет свыше 65,000 узлов. Этих больших сетей может быть до 16,384. Сети класса B вероятно подходять для больших организаций, таких как деловые или государственные агентства.

Сети класса C маленькие, и могут иметь только до 254 узлов, но общее количество сетей класса C превышает 2 миллиона (точнее 2,097,152). Сети, подключаемые к интернет, обычно являются сетями класса C.

Некоторые важные замечания относительно IP адресов:

Класс может быть легко определен по полю1:

поле1 = 1-126: Класс A

поле1 = 128-191: Класс B

поле1 = 192-223: Класс C

(непоказанные значения зарезервированы для специального использования)

- ID узла может иметь любые значения полей кроме всех полей, установленных в 0 или всех полей установленных в 255, так как эти значения зарезервированы для специального использования.

11.3 Маски подсетей



Определение: Маска похожа на IP адрес, но содержит набор битов, которые показывают какая часть IP адреса является идентификатором сети и какая часть идентификатором узла: бит 1 означает "этот бит является частью ID сети" и бит 0 означает "этот бит является частью ID узла."

Маски подсетей *используются для определения подсетей (которые вы получаете, разделяя сеть на маленькие части). Подсети создаются "заимствованием" одного или более бит из части узла.*

Например, рассморим сеть класса С 192.168.1. Для разделения ее на две подсети, вам следует использовать следующую маску:

255.255.255.128

Это легче увидеть, если мы запишем ее в двоичном виде:

11111111. 11111111. 11111111.10000000

В любом адресе класса С, все биты с поля1 по поле3 являются идентификатором сети, имейте в виду, что бит поля4 также включен. Так как этот дополнительный бит имеет только два значения (0 и 1), это означает, что есть две подсети. Каждая подсеть использует оставшиеся 7 бит в поле4 для адресации узлов, в диапазоне от 0 до 127 (вместо обычных 0 - 255 для адресов класса С).

Аналогично, разделяем сеть класса С на четыре подсети следующей маской:

255.255.255.192 или 11111111. 11111111. 11111111.11000000

Два дополнительных бита в поле 4 могут иметь четыре значения (00, 01, 10, 11), таким образом получаем четыре подсети. Каждая подсеть использует оставшиеся шесть бит в поле 4 для адресации узлов в диапазоне 0 - 63.



Иногда маски подсети не определяют дополнительные биты идентификатора сети и, следовательно, не имеют подсетей. Такие маски называют маска подсети по умолчанию. Это следующие маски:

Класс A:	255.0.0.0
Класс B:	255.255.0.0
Класс C:	255.255.255.0

Их называют по умолчанию, потому что они используются при начальной настройке сети, когда нет никаких подсетей.

12 Устранение неисправностей

Этот раздел предлагает действия для решения проблем, с которыми пользователь может столкнуться устанавливая и эксплуатируя RX3042H и инструкции по использованию IP утилит для диагностики проблем.

Если вы не можете решить проблему, свяжитесь с вашим местным дилером.

Проблема	Предлагаемое действие
Индикаторы	
Индикатор Power не горит после включения питания.	Проверьте, что вы используете блок питания, поставляемый с устройством и убедитесь, что он надежно подключен к RX3042H и розетке питания.
Индикатор LINK WAN после подключения Ethernet-кабеля.	Проверьте, что кабель надежно подключен к Ethernet-порту вашего ADSL или кабельного модема и к WAN-порту RX3042H. Удостоверьтесь, что ваш ADSL или кабельный модем включен. Подождите 30 секунд, пока RX3042H установит соединение с вашим модемом.
Индикатор LINK LAN LED после подключения Ethernet-кабеля.	Проверьте, что кабель надежно подключен к вашему сетевому хабу или ПК и к RX3042H. Удостоверьтесь, что ПК и/или хаб включены. Проверьте, что ваш кабель соответствует вашей сети. Для сети 100 Мбит/сек (100BaseTx) следует использовать кабели категории 5. Для сети 10Мбит/сек можно использовать кабели более низкого качества..
Доступ к Интернет	
ПК не имеет доступа к Интернет	Используйте утилиту ping, обсуждаемую в следущем разделе, для проверки возможности связи между PC и RX3042H (по умолчанию IP адрес 192.168.1.1). Если нет связи - проверьте кабель. Если вы используете статический IP адрес для компьютера, (не публичный адрес), проверьте следущее: • Проверьте, что IP адрес шлюза на компьютере является IP адресом RX3042H (смотрите инструкции по просмотру IP информации в руководстве по быстрой установке часть 2.) Если нет, скорректируйте адрес или установите для ПК динамический IP адрес.

Проблема	Предлагаемое действие
ПК не имеет доступа к Интернет (продолжение)	• С помощью вашего провайдера проверьте правильность адреса сервера DNS для вашего ПК. Скорректируйте адрес или настройте ПК для приема этой информации автоматически. • Проверьте, определено ли правило NAT для трансляции частного адреса в публичный IP адрес. Назначенный IP адрес должен быть в пределах диапазона, определенного в правилах NAT. Или настройте ПК для получения адреса с другого устройства (смотрите раздел 3.2 “часть 2 — Настройка ваших компьютеров”). Конфигурация по умолчанию имеет правила NAT для всех динамически назначаемых адресов из пула.
ПК не показывает веб-страницы в Интернет	Проверьте, что сервер DNS, определенный в вашем ПК является правильным для вашего провайдера, как обсуждалось в пункте выше. Вы можете использовать утилиту ping, обсуждаемую в следущем разделе, для проверки связи с сервером DNS вашего провайдера.
Программа менеджер конфигурации	
Вы забыли/потеряли имя пользователя/пароль для менеджера конфигурации	Если вы не изменяли пароль по умолчаню, попробуйте использовать “admin” как имя пользователя и “admin” как пароль. В противном случае вы можете сбросить устройство к заводским параметрам, инструкции предоставлены в разделе 10.7.1 “Восстановление заводских параметров устройства”. ВНИМАНИЕ: Сброс устройства удалит любые установленные параметры и вернет их к значениям по умолчанию.
Невозможно подключиться к менеджеру конфигурации	Используйте утилиту ping, обсуждаемую в следущем разделе, для проверки возможности связи между ПК и сетевым IP адресом RX3042H (по умолчанию 192.168.1.1). Если нет связи - проверьте кабель. Проверьте, что вы используете Internet Explorer 6.0 или новее. На вашем браузере должна быть включена поддержка для Javascript®. Также требуется поддержка для Java®. Проверьте, что IP адрес ПК находится в одной подсети с IP адресом RX3042H.
Изменения для менеджера конфигурации не были установлены	При сохранении любых изменений, удостоверьтесь, что вы нажали кнопку "Apply".

12.1 Диагностика проблем, используя IP утилиты

12.1.1 ping

Ping- команда, которую вы можете использовать для проверки связи между вашим ПК и другими компьютерами вашей сети или интернет. Команда ping посылает сообщение определенному компьютеру. Если компьютер получает сообщение, то посылает ответное сообщение. Для использования этого, вы должны знать IP адрес компьютера с которым вы хотите соединиться.

В компьютерах на основе Windows, вы можете запустить команду ping в меню Пуск. Нажмите на кнопку Пуск, и затем нажмите Выполнить. В открывшемся окне, введите команду типа следующей:

ping 192.168.1.1

Нажмите **OK**. Вы можете использовать любой IP адрес в вашей сети или IP адрес в Интернет.

Если удаленный компьютер принял сообщение, появится окно как показано на рис. 12.1.

```
Command Prompt

C:\Documents and Settings\Alan>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Documents and Settings\Alan>_
```

Рис. 12.1. Использование команды ping

Если удаленный компьютер не найден, вы получите сообщение “Request timed out.”

Используя команду ping, вы можете проверить есть ли связь с RX3042H (используя адрес по умолчанию 192.168.1.1) или адрес, который вы назначили.

Также вы можете проверить, работает ли доступ к интернет, набрав внешний адрес, например для www.yahoo.com (216.115.108.243). Если вы не знаете IP адрес местоположения, вы можете использовать команду nslookup, как объяснено в следующем разделе.

В большинстве других операционных систем с поддеркой IP, вы можете выполнить ту же самую команду в командной строке или через утилиту администрирования.

12.1.2 nslookup

Вы можете использовать команду nslookup для определения IP адреса, связанного с названием сайта. Вы указываете имя, и команда nslookup ищет имя на вашем DNS сервере (обычно располагается у вашего провайдера). Если имя не найдено в DNS таблице вашего провайдера, запрос будет послан другому DNS серверу, и так далее, пока не будет найден. Сервер возвращает связанный с именем IP адрес.

В компьютерах на основе Windows, вы можете запустить команду nslookup в меню Пуск. Нажмите на кнопку Пуск, и затем нажмите Выполнить. В открывшемся окне, введите команду типа следующей:

nslookup

Нажмите **OK**. Появится приглашение к вводу команды (>). Введите, интересующее вас имя, как например www.absnews.com.

В окне отобразится соответствующий IP адрес, как показано на рис. 12.2.

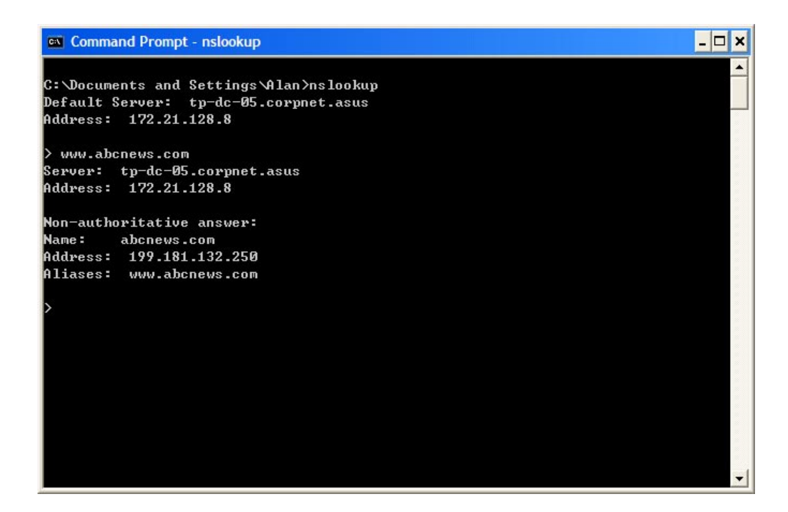


Рис. 12.2. Использование команды nslookup

Одно имя может иметь несколько адресов. Это характерно для вебсайтов, которые имеют интенсивный трафик; они используют несколько серверов с одинаковой информацией.

Для выхода из утилиты nslookup наберите exit и нажмите <Enter>.

13 Индекс